

PAUL J. GELLER
ROBBINS GELLER RUDMAN & DOWD
LLP
120 E. Palmetto Park Road, Suite 500
Boca Raton, Florida 33432
(561) 750-3000
pgeller@rgrdlaw.com

ADAM J. LEVITT
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLC
55 West Monroe Street, Suite 1111
Chicago, Illinois 60603
(312) 984-0000
levitt@whafh.com

BEN BARNOW
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, Illinois 60602
(312) 621-2000
b.barnow@barnowlaw.com

BRIAN R. STRANGE (103252)
STRANGE & CARPENTER
12100 Wilshire Boulevard, Suite 1900
Los Angeles, California 90025
(310) 207-5055
lacounsel@earthlink.net

DAVID A. MCKAY
LAW OFFICES OF DAVID A. MCKAY LLC
555 North Point Center East, Suite 400
Alpharetta, Georgia 30022
(678) 366-5180
david@damckaylaw.com

Plaintiffs' Steering Committee

TIMOTHY G. BLOOD (149343)
BLOOD HURST & O'REARDON, LLP
600 B Street, Suite 1550
San Diego, California 92101
(619) 338-1100
tblood@bholaw.com

GAYLE M. BLATT (122048)
CASEY GERRY SCHENK FRANCAVILLA
BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, California 92101
(619) 238-1811
gmb@cglaw.com

Plaintiffs' Co-Liaison Counsel

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

In re: SONY GAMING NETWORKS AND
CUSTOMER DATA SECURITY BREACH
LITIGATION

) MDL No.: 3:11-md-02258-AJB-MDD

) CLASS ACTION

This Document Pertains To: All Actions

) FIRST AMENDED CONSOLIDATED
) CLASS ACTION COMPLAINT

) JUDGE: The Honorable Anthony J. Battaglia
) CTRM: 12

) JURY TRIAL DEMANDED

1 Plaintiffs Scott Lieberman, Kyle Johnson, Arthur Howe, Adam Schucher, Rebecca Mitchell,
 2 Christopher Wilson, James Wright, Robert Bova, Christian Kallad, Christopher Munsterman, and
 3 Timothy Whyland, individually and on behalf of all others similarly situated, upon personal
 4 knowledge of the facts pertaining to them and on information and belief as to all other matters, by
 5 and through Plaintiffs' Steering Committee and Plaintiffs' Co-Liaison Counsel, bring this First
 6 Amended Consolidated Class Action Complaint against Sony Computer Entertainment America,
 7 LLC ("SCEA"); Sony Network Entertainment America, Inc. ("SNEA"); Sony Online Entertainment
 8 LLC ("SOE LLC"); and Sony Network Entertainment International, LLC ("SNEI")(collectively,
 9 "Defendants" or "Sony").

10 INTRODUCTION

11 1. This First Amended Consolidated Class Action Complaint (the "Complaint") is filed
 12 pursuant to the August 8, 2011 Transfer Order of the Judicial Panel on Multidistrict Litigation
 13 ("JPML"), and Order Following PSC Status Conference, ¶1 [Dkt. No. 63], and presents claims
 14 brought against Defendants in the separate cases filed in this District or transferred to this District by
 15 the JPML. Unless otherwise ordered by the Court, all claims presented in any case against
 16 Defendants subsequently made a part of this multidistrict litigation proceeding shall be deemed to be
 17 included in this Complaint.

18 2. This Complaint is filed to promote judicial efficiency and economy in the
 19 adjudication and resolution of pretrial matters and is not intended to effect consolidation for trial of
 20 the transferred cases. Neither is this Complaint intended to change the rights of the parties, nor to
 21 make those who are the plaintiffs in one case the plaintiffs in another. *See In re Propulsid Prods.*
 22 *Liab. Litig.*, 208 F.R.D. 133, 140-42 (E.D. La. 2002).

23 3. For their own commercial and financial benefit, Defendants solicited and collected
 24 their customers' sensitive personal and financial information, including credit and debit card
 25 numbers. However, they failed to reasonably maintain this information in a secure manner, in
 26 violation of their duties to do so, in breach of their express agreements to do so, and contrary to the
 27 reasonable expectations of consumers. Further, Defendants failed to disclose to its customers at the
 28 time they purchased gaming consoles and again when they signed up for products and services

1 offered by Defendants, that Defendants would not bother to maintain their customers' information in
2 a reasonable manner. This failure violated minimum and reasonable industry-standard security
3 measures, directly leading to and permitting one of the largest data security breaches in history,
4 directly affecting upwards of over 50 million consumers in the United States and Canada, and an
5 additional estimated 20 to 30 million consumers worldwide. Plaintiffs and the other members of the
6 proposed class and subclasses ("Class members"), as a matter of law, were entitled to rely on Sony
7 to not violate its duty to reasonably secure the concerned personal information.

8 4. In April 2011, Sony sustained one or more massive security breaches to its computer
9 systems, servers, and databases ("Network"), that otherwise would not have occurred, or would not
10 have occurred with such severity, but for Sony's failure to maintain adequate, reasonable and
11 industry-standard data security, a failure that represents gross disregard for the common law and
12 other duties and obligations Sony was under.

13 5. These security breaches (collectively, the "Data Breach"), placed the sensitive
14 personal and financial information of Plaintiffs and the other Class members in the hands of cyber
15 criminals, including customer names, mailing addresses, email addresses, and birth dates, as well as
16 credit and debit card numbers, expiration dates, security codes, online network passwords, login
17 credentials, answers to security questions, and other personal information (collectively, "Personal
18 Information").

19 6. Plaintiffs and the other Class members provided their Personal Information to Sony
20 when registering/subscribing to the PlayStation Network ("PSN"), Qriocity, and/or Sony Online
21 Entertainment ("SOE") (collectively, "Sony Online Services"), and, upon information and belief,
22 Sony kept that Personal Information on its Network in perpetuity, regardless of whether a Sony
23 customer inactivated or terminated their Sony Online Services account(s).

24 7. Further, on information and belief, Sony failed to adequately or properly separate
25 Plaintiffs' and the other Class members' Personal Information, in effect, allowing its bundling or
26 commingling in such a fashion as to make the information available to entities not authorized or
27 intended by Plaintiffs and the other Class members and, further, aiding the unlawful access of the
28 Personal Information to unauthorized persons, including those initiating and completing the Data

1 Breach. Through such conduct, Sony allowed access to the Personal Information to those who did
2 not have a lawful and permissible purpose.

3 8. Sony owed a legal duty to Plaintiffs and the other Class members to maintain
4 reasonable, adequate and industry-standard security measures to secure, protect, and safeguard their
5 Personal Information stored on its Network. This legal duty arose from the facts and circumstances
6 surrounding Sony's solicitation and collection of the information, express promises by Defendants
7 (either directly or indirectly), the reasonable expectations of the consumers and through the
8 omissions, acts and representations of Defendants. Sony breached these duties by failing to design
9 and implement appropriate firewalls and computer systems, failing to properly and adequately
10 encrypt data, and unnecessarily storing and retaining Plaintiffs' and the other Class members'
11 Personal Information on its inadequately-protected Network. Sony did not act in a commercially
12 reasonable manner.

13 9. Moreover, maintaining reasonable, adequate, and industry-standard security measures
14 to protect the Personal Information of millions of customers is an expensive proposition. But rather
15 than do what is reasonable and expected in the world of online commerce, Sony, one of the largest
16 and wealthiest electronics companies in the world, only maintained grossly inadequate security,
17 saving significantly on the costs of providing reasonably adequate security and foisting unnecessary
18 risk to Sony's customers.

19 10. Sony was aware of the security vulnerabilities of its Network well before the Data
20 Breach, yet failed to warn Plaintiffs and the other Class members of those risks and the susceptibility
21 of its Network to unlawful and unauthorized access, such as the Data Breach here; failed to remedy
22 known defects in its Network that made it vulnerable to the Data Breach; and continued to encourage
23 consumers to buy Sony hardware and to subscribe to the Sony Online Services without warning
24 consumers about the risks inherent in purchasing and relying on Sony's inadequate data security.

25 11. Sony knew or should have known that its inadequate security systems placed Sony at
26 an increased risk for the Data Breach, which directly and proximately caused the theft of Plaintiffs'
27 and the other Class members' Personal Information and the month-long interruption of Sony Online
28 Services.

1 12. On information and belief:

2 (a) Sony took numerous precautions and spent substantial funds to secure its
3 proprietary-development server containing its own sensitive information, including the installation of
4 appropriate firewalls, IP address limitations and updated software, but recklessly declined to provide
5 adequate protections for Plaintiffs' and the other Class members' Personal Information;

6 (b) Sony implemented enhanced measures for its own proprietary systems but
7 failed to provide said measures to Plaintiffs' and the other Class members' Personal Information, and
8 these disparities existed because Sony chose to allocate resources to protect itself and its entities, a
9 desire that resulted in inadequate funding and effort to protect Plaintiffs' and the other Class
10 members' Personal Information;

11 (c) Sony's conduct led to the conclusion that protecting its own development
12 server was Sony's "number one concern;"

13 (d) Sony chose to not install an appropriate firewall on the Network, and
14 implemented firewalls on an *ad-hoc* and inadequate basis when it determined that a particular user
15 was attempting to gain unauthorized access;

16 (e) Sony sought to cut its costs at the expense of Plaintiffs and the other Class
17 members by terminating a significant number of employees prior to the security breach, including
18 personnel responsible for maintaining the security of the Plaintiffs' and the other Class members'
19 Personal Information; and

20 (f) Sony's gaming consoles have the same access number, rendering them more
21 prone to data breaches since access to a single unit provides access to all.

22 13. According to Confidential Witness 1, a former Sony employee who was with SCEA
23 from 2006 to 2008, and with Sony Online Entertainment April 2010 to August 2010, Sony invested
24 significant resources, including firewalls, a debug unit and IP address limitations, to protect its own
25 confidential proprietary information housed on Sony's "development server," known internally as
26 "the PS DevNetwork." According to this witness, these measures made it "extremely difficult" to
27 breach the PS DevNetwork. While Sony knew that these basic security measures were necessary to
28 protect its proprietary systems, it chose to cut corners when it came to its customers' Personal

1 Information and failed to implement similar safeguards on the PSN. The PSN at important and
2 critical times lacked basic security measures such as updated software, adequate encryption and
3 firewalls. As a direct result of Sony's failure to adequately protect Plaintiffs' and the other Class
4 members' data, hackers were able to improperly access and steal their Personal Information on an
5 epic scale.

6 14. At the same time as Sony was saving money by maintaining substandard data security
7 for its Network and for Sony Online Services, Sony was also earning significant amounts of money
8 from Sony Online Services. Sony provides Sony Online Services to Plaintiffs and the other Class
9 members because it enables Sony to make money from those Class members through increased sales
10 of Sony hardware, increased sales of Sony software, sales of Sony Online Services subscriptions,
11 and sales of Sony Online Services in-game downloads or "add-ons." Sony did not need to collect
12 Plaintiffs' and the other Class members' Personal Information in the course of making Sony Online
13 Services available to make money in any of these ways – Sony could have continued to sell
14 hardware, software, subscriptions, and downloads without requiring Plaintiffs and the other Class
15 members to personally identify themselves and without recklessly storing their Personal Information
16 as Sony did on Sony's Network. Sony demanded and kept Plaintiffs' and the other Class members'
17 Personal Information as a condition for accessing Sony Online Services.

18 15. Sony obtains additional revenue, though this time from third-parties rather than from
19 Plaintiffs and the other Class members directly, by selling targeted PSN in-game advertising space to
20 those third-parties, enabling Sony to show Plaintiffs and the other Class members ads when they
21 play games on their Sony devices that incorporate dynamic advertisement serving technology. Sony
22 did not need to collect and store Plaintiffs' and the other Class members' Personal Information to
23 obtain revenue selling advertising space – Sony could have sold dynamic advertising space to third
24 parties without requiring Plaintiffs and the other Class members to personally identify themselves
25 and without recklessly storing their Personal Information as Sony did on the Network.

26 16. As the result of Sony's failure to reasonably and adequately secure its Network, the
27 Data Breach occurred and Plaintiffs' and the other Class members' Personal Information was
28 compromised, placing them at an increased risk of fraud and identity theft, and causing direct

1 financial expenses associated with credit monitoring, replacement of compromised credit, debit and
2 bank card numbers, and other measures needed to protect against fraud arising from the Data Breach.
3 Plaintiffs and the other Class members were also deprived of the unencumbered use of their
4 passwords, which were obtained by a third party without their consent as the result of Sony's failure
5 to adequately and reasonably secure Plaintiffs' and the other Class members' Personal Information.

6 17. Additionally, because of its inadequate security and the resulting Data Breach, Sony
7 shut down Sony Online Services for several weeks, causing further damage to Plaintiffs and the
8 other Class members, including the loss of use of Sony Online Services and the full functionality of
9 hardware, including Sony PlayStation 3 ("PS3") consoles and PlayStation Portable ("PSP") devices
10 and related software and games ("Equipment"), as well as "add-ons" Plaintiffs and the other Class
11 members paid Sony money for and could only use when Sony Online Services were, in-fact, on-line.
12 While Sony Online Services were turned off, Plaintiffs and the other Class members continued to be
13 charged for prepaid subscriptions to products or services for specified periods of time accessible
14 through the Network, including, but not limited to Netflix, MLB.TV, and NHL Gamecenter LIVE
15 ("Third-Party Services"), despite the inability to use such Third-Party Services.

16 PARTIES

17 *Plaintiffs*

18 18. Robert M. Bova ("Bova") resides in Tewksbury, Middlesex County, Massachusetts.
19 Plaintiff Bova acquired a PS3 in or around 2008 and created a PSN account using his PS3 in or
20 around 2009. In order to create his PSN account, Plaintiff Bova provided the following personal
21 information to Sony: name, gender, date of birth, mailing address, e-mail address, phone number,
22 and, possibly, information regarding his Bank of America Visa and TD Bank debit card accounts,
23 including the card numbers, expiration dates, security codes, and billing address. Plaintiff Bova used
24 the PSN through his PS3 to play games online and to download additional game content such as map
25 packs. Plaintiff Bova's PSN account was active on April 16, 2011, and at all relevant times
26 thereafter. Plaintiff Bova first learned that his Personal Information had been compromised by the
27 Data Breach through online news sources. As a result of the Data Breach: (a) Plaintiff Bova's
28

1 Personal Information was stolen, exposing him to a greater risk of identity theft and fraud; (b)
2 Plaintiff Bova was unable to access the PSN for approximately four weeks; and (c) Plaintiff Bova
3 purchased credit monitoring services for approximately \$10 per month. Plaintiff Bova had a
4 reasonable expectation that the Network was secure, was not told until after the Data Breach that the
5 Network was not secure, and reasonably believed that Sony would take all reasonable measures to
6 protect his Personal Information from theft consistent with industry standards.

7 19. Christian Pierce Kalled ("Kalled") resides in Wolfeboro, Carroll County, New
8 Hampshire. Plaintiff Kalled acquired a PS3 in or around October 2009. On or about October 21,
9 2009, Plaintiff Kalled created a PSN account using his PS3. In order to create his PSN account,
10 Plaintiff Kalled provided the following personal information to Sony: name, gender, date of birth,
11 mailing address, e-mail address, phone number, and, possibly, information regarding his American
12 Express credit card account, including the card number, expiration date, security code, and billing
13 address. Plaintiff Kalled used the PSN through his PS3 to play games online, to download game
14 updates, to browse the internet, and to stream prepaid media content from Netflix. Plaintiff Kalled's
15 PSN account, as well as his Netflix account, were all active on April 16, 2011, and at all relevant
16 times thereafter. Plaintiff Kalled first learned that his Personal Information had been compromised
17 by the Data Breach on May 25, 2011 from an online news article. As a result of the Data Breach: (a)
18 Plaintiff Kalled's Personal Information was stolen, exposing him to a greater risk of identity theft
19 and fraud; and (b) Plaintiff Kalled was unable to access the PSN and prepaid Netflix service through
20 the PSN for approximately three weeks. Although Kalled did technically have access to his Netflix
21 account on his personal computer during the time the PSN was down (April 20, 2011 through May
22 14, 2011), Kalled still suffered injury as a result of not being able to use his prepaid Netflix account
23 through the PSN. This is so because Kalled's intent in purchasing Netflix was to be able to stream
24 movies for viewing on his home television through the PSN. Kalled would not have paid for a
25 Netflix account in the first instance if he had to watch streamed movies on a small computer
26 monitor, as opposed to his large screen television. Plaintiff Kalled had a reasonable expectation that
27 the Network was secure, was not told until after the Data Breach that the Network was not secure,
28

1 and reasonably believed that Sony would take all reasonable measures to protect his Personal
2 Information from theft consistent with industry standards.

3 20. Scott Lieberman ("Lieberman") resides in Plantation, Broward County, Florida.
4 Plaintiff Lieberman acquired a PS3 in or around early 2007, and created a PSN account shortly
5 thereafter. In order to create his PSN account, Plaintiff Lieberman provided the following personal
6 information to Sony: name, gender, date of birth, mailing address, e-mail address, phone number,
7 and information regarding his American Express credit card account, including the card number,
8 expiration date, security code, and billing address. Plaintiff Lieberman used the PSN to play single
9 and multi-player games online with other PSN users, to purchase and download games, stream
10 prepaid media content from Netflix, and to chat with friends who also used the PSN. Plaintiff
11 Lieberman's PSN account and Netflix account were active on April 16, 2011, and at all relevant
12 times thereafter. Plaintiff Lieberman first learned that his Personal Information had been
13 compromised by the Data Breach through Internet media in or around mid-April 2011. As a result of
14 the Data Breach: (a) Plaintiff Lieberman's Personal Information was stolen, exposing him to a
15 greater risk of identity theft and fraud; and (b) Plaintiff Lieberman was unable to access the PSN,
16 including prepaid Netflix streaming services through the PSN, for approximately 30 days. Plaintiff
17 Liebermann had a reasonable expectation that the Network was secure, was not told until after the
18 Data Breach that the Network was not secure, and reasonably believed that Sony would take all
19 reasonable measures to protect his Personal Information from theft consistent with industry
20 standards. Had Lieberman known that Sony did not have adequate data security in place to protect
21 his Personal Information from theft, and that the security of the Network was not consistent with
22 industry standards, he would not have paid as much money as he did for his PS3, if at all.

23 21. Kyle Johnson ("Johnson") resides in San Diego, San Diego County, California.
24 Plaintiff Johnson acquired a PS3 in or around the summer of 2007, and created a PSN account
25 shortly thereafter. In order to create his PSN account, Plaintiff Johnson provided the following
26 personal information to Sony: name, gender, date of birth, mailing address, e-mail address, phone
27 number, and credit card information, including the card number, expiration date, security code, and
28 billing address. Plaintiff Johnson has provided such credit card information to Sony regarding three

1 separate credit card accounts—Discover, American Express, and Visa. Plaintiff Johnson used the
 2 PSN to play single and multi-player games online with other PSN users, purchase and download
 3 games, stream prepaid media content from Netflix, and to browse the Internet. Plaintiff Johnson’s
 4 PSN account and Netflix account were active on April 16, 2011, and at all relevant times thereafter.
 5 Plaintiff Johnson first learned that his Personal Information had been compromised by the Data
 6 Breach through media coverage of the Data Breach and later through an email he received from
 7 Sony dated April 27, 2011, regarding the incident. As a result of the Data Breach: (a) Plaintiff
 8 Johnson’s Personal Information was stolen, exposing him to a greater risk of identity theft and fraud;
 9 and (b) Plaintiff Johnson was unable to access the PSN, including prepaid Netflix streaming
 10 services, for approximately 30 days. In or around October 2011, two unauthorized charges appeared
 11 on Plaintiff Johnson’s Visa card. Plaintiff Johnson had a reasonable expectation that the Network
 12 was secure, was not told until after the Data Breach that the Network was not secure, and reasonably
 13 believed that Sony would take all reasonable measures to protect his Personal Information from theft
 14 consistent with industry standards. Plaintiff Johnson suffered injury in fact and lost money or
 15 property as a result of the acts and omissions alleged. .

16 22. Arthur Howe (“Howe”) resides in San Diego, San Diego County, California. Plaintiff
 17 Howe acquired a PS3 in or around 2008 and created two new PSN accounts – one for him and one
 18 for his minor son. In order to create his PSN accounts, Plaintiff Howe provided the following
 19 personal information regarding himself to Sony: name, date of birth, mailing address, email address,
 20 phone number, and information regarding his Union Bank debit/credit account and his son’s
 21 mother’s US Bank account, including the card numbers, expiration dates, security codes, and billing
 22 addresses. Plaintiff Howe used the PSN mainly to play single and multi-player games online with
 23 other PSN users. Plaintiff Howe also used the PSN to purchase and download “map packs,” and to
 24 stream prepaid media content from Netflix. Plaintiff Howe’s PSN accounts and Netflix account were
 25 all active on April 16, 2011, and at all relevant times thereafter. Plaintiff Howe first learned that his
 26 Personal Information had been compromised by the Data Breach through a letter from Sony dated
 27 April 28, 2011. As a result of the Data Breach: (a) Plaintiff Howe’s Personal Information was stolen,
 28 exposing him to a greater risk of identity theft and fraud; (b) Plaintiff Howe was unable to access the

1 PSN, including prepaid Netflix streaming service for which he was billed \$8.99 per month, for
2 approximately 30 days; (c) Plaintiff Howe was forced to close two bank accounts that were
3 compromised; and (d) Plaintiff Howe was forced to purchase a credit monitoring service from
4 freecreditreport.com at a cost of \$9.00 per month. Plaintiff Howe had a reasonable expectation that
5 the Network was secure, was not told until after the Data Breach that the Network was not secure,
6 and reasonably believed that Sony would take all reasonable measures to protect his Personal
7 Information from theft consistent with industry standards. Plaintiff Howe suffered injury in fact and
8 lost money or property as a result of the acts and omissions alleged.

9 23. Christopher Munsterman (“Munsterman”) resides in Kansas City, Jackson County,
10 Missouri. Plaintiff Munsterman acquired a PS3 and created a PSN account using his PS3 in or
11 around 2008. In order to create his PSN account, Plaintiff Munsterman provided the following
12 personal information to Sony: name, gender, date of birth, mailing address, e-mail address, phone
13 number, and, possibly, information regarding his Commerce Visa debit card account, including the
14 card number, expiration date, security code, and billing address. Plaintiff Munsterman used the PSN
15 through his PS3 to play games online, to download games and movies, to browse the internet, to chat
16 with friends, and to stream prepaid media content from Netflix. Plaintiff Munsterman’s PSN
17 account, as well as his Netflix account, were both active on April 16, 2011, and at all relevant times
18 thereafter. Plaintiff Munsterman first learned that his Personal Information had been compromised
19 by the Data Breach through an email he received on May 27, 2011. As a result of the Data Breach:
20 (a) Plaintiff Munsterman’s Personal Information was stolen, exposing him to a greater risk of
21 identity theft and fraud; and (b) Plaintiff Munsterman was unable to access the PSN and prepaid
22 Netflix service through the PSN for approximately three weeks. Although Munsterman did
23 technically have access to his Netflix account on his personal computer during the time the PSN was
24 down (April 20, 2011 through May 14, 2011), Munsterman still suffered injury as a result of not
25 being able to use his prepaid Netflix account through the PSN. This is so because Munsterman’s
26 intent in purchasing Netflix was to be able to stream movies for viewing on his home television
27 through the PSN. Munsterman would not have paid for a Netflix account in the first instance if he
28 had to watch streamed movies on a small computer monitor, as opposed to his large screen

1 television. Plaintiff Munsterman had a reasonable expectation that the Network was secure, was not
2 told until after the Data Breach that the Network was not secure, and reasonably believed that Sony
3 would take all reasonable measures to protect his Personal Information from theft consistent with
4 industry standards.

5 24. Adam Schucher ("Schucher") resides in Surfside, Miami-Dade County, Florida.
6 Plaintiff Schucher acquired a PS3 in or around mid-2008 and created a PSN account shortly
7 thereafter. In order to create his PSN account, Plaintiff Schucher provided the following personal
8 information to Sony: name, gender, date of birth, mailing address, e-mail address, phone number,
9 and information regarding his Citibank Visa credit card account, including the card number,
10 expiration date, security code, and billing address. Plaintiff Schucher used the PSN mainly to
11 purchase and download karaoke songs for *Karaoke Revolution Presents: American Idol* and to chat
12 with friends who also used the PSN. Plaintiff Schucher's PSN account was active on April 16, 2011,
13 and at all relevant times thereafter. Plaintiff Schucher first learned that his Personal Information had
14 been compromised by the Data Breach through Internet media on or around mid-April 2011. As a
15 result of the Data Breach: (a) Plaintiff Schucher's Personal Information was stolen, exposing him to
16 a greater risk of identity theft and fraud; and (b) Plaintiff Schucher was unable to access the PSN for
17 approximately 30 days. Plaintiff Schucher had a reasonable expectation that the Network was
18 secure, was not told until after the Data Breach that the Network was not secure, and reasonably
19 believed that Sony would take all reasonable measures to protect his Personal Information from theft
20 consistent with industry standards. Had Plaintiff Schucher known that Sony did not have adequate
21 data security in place to protect his Personal Information from theft, and that the security of the
22 Network was not consistent with industry standards, he would not have paid as much money as he
23 did for his PS3, if at all.

24 25. Rebecca Mitchell ("Mitchell") resides in East Lansing, Ingham County, Michigan.
25 Plaintiff Mitchell acquired a PS3 in or around May 2009 and created a PSN account. In creating her
26 account, Plaintiff Mitchell provided the following personal information to Sony: name, gender, date
27 of birth, mailing address, e-mail address, and phone number. Subsequently thereto and prior to April
28 2011, Plaintiff Mitchell provided the PSN with financial information relating to her mother's credit

1 card and her own Visa debit card account, including the card numbers, expiration dates, security
2 codes, and billing addresses. Plaintiff Mitchell used the PSN mainly to purchase, download, and/or
3 access games, karaoke songs for the PlayStation game *Sing Star*, and to browse the Internet. Plaintiff
4 Mitchell's PSN account was active on April 16, 2011, and at all relevant times thereafter. Plaintiff
5 Mitchell first learned that her Personal Information had been compromised by the Data Breach
6 through Internet media on or around April 19, 2011. As a result of the Data Breach: (a) Plaintiff
7 Mitchell's Personal Information was stolen, exposing her to a greater risk of identity theft and fraud;
8 and (b) Plaintiff Mitchell was unable to access the PSN for approximately 30 days. Plaintiff Mitchell
9 had a reasonable expectation that the Network was secure, was not told until after the Data Breach
10 that the Network was not secure, and reasonably believed that Sony would take all reasonable
11 measures to protect his Personal Information from theft consistent with industry standards. Had
12 Mitchell known that Sony did not have adequate data security in place to protect her Personal
13 Information from theft, and that the security of the Network was not consistent with industry
14 standards, she would not have paid as much money as she did for his PS3, if at all.

15 26. Christopher Wilson ("Wilson") resides in Dallas, Dallas County, Texas. Plaintiff
16 Wilson acquired a PS3 on or around January 2007 and created a PSN account shortly thereafter. In
17 order to create his PSN account, Plaintiff Wilson provided the following personal information to
18 Sony: name, gender, date of birth, mailing address, e-mail address, phone number, and information
19 regarding his Chase Bank Visa debit card account, including the card number, expiration date,
20 security code, and billing address. Plaintiff Wilson used the PSN mainly to play games online with
21 other PSN users, to purchase and download games, and to stream prepaid media content from
22 Netflix. Plaintiff Wilson's PSN account and Netflix account were active on April 16, 2011, and at all
23 relevant times thereafter. Plaintiff Wilson first learned that his Personal Information had been
24 compromised by the Data Breach through an email he received from Sony on or around April 27,
25 2011. As a result of the Data Breach: (a) Plaintiff Wilson's Personal Information was stolen,
26 exposing him to a greater risk of identity theft and fraud; and (b) Plaintiff Wilson was unable to
27 access the PSN or prepaid Netflix service through the PSN for approximately 30 days. Plaintiff
28 Wilson had a reasonable expectation that the Network was secure, was not told until after the Data

1 Breach that the Network was not secure, and reasonably believed that Sony would take all
2 reasonable measures to protect his Personal Information from theft consistent with industry
3 standards. Had Wilson known that Sony did not have adequate data security in place to protect his
4 Personal Information from theft, and that the security of the Network was not consistent with
5 industry standards, he would not have paid as much money as he did for his PS3, if at all.

6 27. James Wright ("Wright") resides in Columbus, Franklin County, Ohio. Plaintiff
7 Wright acquired a PS3 in or around 2008. Several years ago, Plaintiff Wright created an SOE
8 account, a Qriocity account and, in or around 2008 or 2009, a PSN account. In order to create his
9 SOE, Qriocity and PSN accounts, Plaintiff Wright provided the following personal information to
10 Sony: name, gender, date of birth, mailing address, e-mail address, phone number, and information
11 regarding his Visa US Bank Debit / Credit Card account, including the card number, expiration date,
12 security code, and billing address. Plaintiff Wright used his PS3 to play DC Universe Online through
13 his SOE account. Plaintiff Wright used his PS3 to play music through his Qriocity account.
14 Plaintiff Wright used the PSN to play games online, to purchase and download games, and to stream
15 prepaid media content from Netflix. Plaintiff Wright's PSN, SOE, and Qriocity accounts, as well as
16 his Netflix account, were all active on April 16, 2011, and at all relevant times thereafter. Plaintiff
17 Wright first learned that his Personal Information had been compromised by the Data Breach
18 through a conversation with friends. As a result of the Data Breach: (a) Plaintiff Wright's Personal
19 Information was stolen, exposing him to a greater risk of identity theft and fraud; and (b) Plaintiff
20 Wright was unable to access the PSN, prepaid Netflix service through the PSN, his SOE account,
21 and his Qriocity account for approximately three weeks. Plaintiff Wright had a reasonable
22 expectation that the Network was secure, was not told until after the Data Breach that the Network
23 was not secure, and reasonably believed that Sony would take all reasonable measures to protect his
24 Personal Information from theft consistent with industry standards. Had Wright known that Sony did
25 not have adequate data security in place to protect his Personal Information from theft, and that the
26 security of the Network was not consistent with industry standards, he would not have paid as much
27 money as he did for his PS3, if at all

28

1 28. Timothy B. Whyland (“Whyland”) resides in Baldwinsville, Onondaga County, New
2 York. Plaintiff Whyland acquired a PS3 and created a PSN account in or around 2009 using his PS3.
3 In order to create his PSN account, Plaintiff Whyland provided the following personal information to
4 Sony: name, gender, date of birth, mailing address, e-mail address, phone number, and information
5 regarding his debit card account, including the card number, expiration date, security code, and
6 billing address. Plaintiff Whyland used the PSN through his PS3 to play games online, and to
7 download game updates, including additional golf courses for Tiger Woods’ Golf Masters PGA Tour
8 2012 and maps for Battlefield Bad Company 2. Plaintiff Whyland’s PSN account was active on
9 April 16, 2011, and at all relevant times thereafter. Plaintiff Whyland first learned that his Personal
10 Information had been compromised by the Data Breach from an online news article after he was
11 unable to access the PSN. As a result of the Data Breach: (a) Plaintiff Whyland’s Personal
12 Information was stolen, exposing him to a greater risk of identity theft and fraud; and (b) Plaintiff
13 Whyland was unable to access the PSN for approximately three weeks. Plaintiff Whyland had a
14 reasonable expectation that the Network was secure, was not told until after the Data Breach that the
15 Network was not secure, and reasonably believed that Sony would take all reasonable measures to
16 protect his Personal Information from theft consistent with industry standards.

17 29. Had Sony not concealed from the public, Plaintiffs, and the other Class members that
18 it failed to employ reasonable, adequate, or industry-standard security measures to protect its
19 customers’ Personal Information, Plaintiffs and the other Class members, as reasonable consumers,
20 would not have purchased their PS3s, would not have paid the same amount for their PS3s, and/or
21 would not have provided their Personal Information to Sony.

22 ***Defendants***

23 30. Sony Computer Entertainment America LLC (“SCEA”) is a Delaware limited
24 liability company with its principal place of business located at 919 East Hillsdale Boulevard, Foster
25 City, California 94404, and conducts business in this District. SCEA is a wholly-owned subsidiary
26 of Sony Corporation of America. On information and belief, SCEA develops, produces, markets,
27 and/or distributes the PS3, PSP, and related hardware and software.

28

31. Sony Network Entertainment America, Inc. (“SNEA”) is a Delaware corporation with its principal place of business located at 550 Madison Avenue, 27th Floor, New York, New York 10022, and conducts business in this District. On information and belief, SNEA functions as Sony’s integrated planner and operator of Internet-based content delivery services to owners of Sony televisions, game machines, and other hardware such as the PS3 and PSP, including collecting and managing the Financial, Personal ID, and User Data for the PSN and Oriocity services.

32. Sony Network Entertainment International LLC (“SNEI”) is a Delaware limited liability company with its principal place of business located at 6080 Center Drive, Los Angeles, California 90045, and conducts business in this District. On information and belief, SNEI functions as an operator of Internet-based content delivery services to owners of Sony televisions, game machines, and other hardware such as the PS3 and PSP, including collecting and managing the Financial, Personal ID, and User Data for PSN and Qriocity services.

33. Sony Online Entertainment LLC (“SOE LLC”) is a Delaware limited liability company with its principal place of business located at 8928 Terman Court, San Diego, California 92121, and conducts business in this District. On information and belief, SOE LLC functions as the integrated planner and operator of Sony’s online and social network games, including collecting and managing the Financial, Personal ID, and User Data for SOE services.

34. Defendants SCNA, SENA, SNEI, and SOE LLC are sometimes collectively referred to herein as “Sony.”

35. At all times relevant to this action, each and every Defendant was an agent or acted with the authority of each and every other Defendant. In doing the things alleged herein, each and every Defendant was acting within the course and scope of this agency or employment and was acting with the consent, permission and authorization of each of the remaining Defendants. All actions of each Defendant, as alleged herein, were ratified and approved by every other Defendant or its officers or managing agents.

JURISDICTION AND VENUE

36. The Court has subject matter jurisdiction over this class action pursuant 28 U.S.C. §1332(d), because Plaintiffs and the other Class members are of diverse citizenship from one or

1 more Defendants, there are more than 100 Class members nationwide, and the aggregate amount in
2 controversy exceeds five million dollars (\$5,000,000.00), excluding interest and costs.

3 37. Venue is proper in this District under 28 U.S.C. §1391 because Defendants engaged
4 in substantial conduct relevant to Plaintiffs' claims within this District and have caused harm to
5 Class members residing within this District. Additionally, the class action lawsuits referenced in the
6 caption above have been transferred to this Court for coordinated or consolidated pretrial
7 proceedings per the Transfer Order of the JPML dated August, 8, 2011. Plaintiffs in the transferred
8 actions reserve their rights of remand to the districts from which they were transferred at or before
9 the conclusion of the pre-trial proceedings.

10 **SUBSTANTIVE FACTUAL ALLEGATIONS**

11 **A. PlayStation Network, Qriocity, and Sony Online Entertainment**

12 38. Sony developed and launched the PlayStation video game console in 1994.
13 Defendants' current version, the PS3, was released in 2006 and has sold over 47.9 million units
14 worldwide.

15 39. In 2004, Sony developed and marketed its PSP, which is a hand-held gaming device.

16 40. One of the key features of the PS3 and PSP devices is their Internet networking
17 capabilities that allow users to connect to the Internet from the devices over a landline connection or
18 "Wi-Fi" – a wireless networking technology allowing the devices to communicate over a wireless
19 signal. As detailed below, the ability of PS3 consoles to access content from the Internet is a key and
20 important part of Sony's business model. It does not merely sell gaming consoles. Instead, Sony's
21 business model is to use the gaming console as a portal to permit PS3 owners to access and pay for
22 content, including games, music and videos, from which Sony and its subsidiaries sell content to its
23 PS3 customers. Sony also has business contracts with other content providers from which it earns
24 revenue. Sony then solicits and collects the Personal Information, sets up accounts and makes it
25 easy for its customers to continue to spend money purchasing content. This aspect of Sony is its
26 most profitable and most valuable.

27 41. Another key feature of the PS3 and PSP is the PlayStation Network ("PSN"). PSN,
28 among other things, allows video game players to engage in multiplayer gaming online (*i.e.*, two

1 individuals can compete against each other in the same video game over an Internet connection as
2 opposed to being in the same room). As of January 25, 2011, PSN had over 69 million registered
3 users worldwide, including Plaintiffs.

4 42. In or around February 2011, Defendants launched an entertainment subscription
5 service called “Qriocity” (pronounced “curiosity”) that allows users to watch videos, stream music,
6 and upload and manage their personal video and music libraries on their PS3, PSP, and other
7 devices.

8 43. In or around 1999, SOE LLC, in conjunction with the other Defendants, began
9 developing a service that provides online interactive role-playing games that allowed individuals to
10 compete against each other in the same video game. As of 2011, SOE had over 24.6 million
11 registered users worldwide, including Plaintiff Wright.

12 44. In addition to serving as an online forum or platform for multiplayer gaming and
13 video/music management, Sony Online Services also comprise an online virtual market where PS3,
14 PSP, and online users can purchase videogames, add-on content (such as “map packs” for popular
15 first person shooter games or karaoke songs for popular singing games), demos, themes, game and
16 movie trailers, TV shows, and movies (“Downloads”). Sony Online Services customers must pay
17 Sony to purchase these Downloads and can use many of them only when they are logged into and
18 using Sony Online Services.

19 45. The PSN also works with various third parties to offer a variety of Third-Party
20 Services – such as Netflix, MLB.TV and NHL Gamecenter LIVE – that can be accessed through the
21 PSN. Many users who subscribe to and pay for these Third-Party Services can only access them
22 through their PSN account.

23 46. As of September 2009, there had been over 600 million downloads from the PSN
24 store. Since its launch in February 2011, PS3 and PSP users have participated in video and music
25 streaming through Qriocity.

26 47. SNEA and SNEI, in conjunction with other Defendants, manage the PSN and
27 Qriocity services, including overseeing the content delivered to PSN and Qriocity users and handling
28

1 and managing the Personal Information provided by Plaintiffs and the other Class members as a part
2 of their membership and usage of the PSN and Qriocity services.

3 48. SOE LLC manages SOE and its services, including overseeing the content delivered
4 to users and managing the Personal Information provided by users as a part of their membership and
5 usage of SOE services.

6 49. When registering with and/or joining PSN, Qriocity, and/or SOE, users are required
7 to establish an account by providing various Personal Information to Sony, which Sony, in turn,
8 stores and maintains on its Network.

9 50. On information and belief, Sony stores this Personal Information on its Network in
10 perpetuity, regardless of whether the Sony Online Services users inactivates or terminates their Sony
11 Online Services account(s).

12 51. Sony continually monitors and records users' activities, purchases, and usage on the
13 PSN, Qriocity, and SOE, and maintains that usage data in various computer databases on its servers.

14 52. Users with an account may also create a subaccount for their minor children and
15 others linked to their primary account. During the registration process for these subaccounts, users
16 are required to provide various Personal Information regarding minor children to Sony, which Sony,
17 in turn, stores and maintains on its Network. Sony continually monitors and records subaccount
18 users' activities, purchases, and usage on PSN, Qriocity, and SOE and maintains that usage data in
19 various computer databases on its servers.

20 53. Users with PSN, Qriocity, and/or SOE accounts may also sign up and pay for Third-
21 Party Services, such as Netflix, to use on their PSP and PS3 devices. On information and belief,
22 Sony allowed Third-Party Services, such as Netflix, access to Plaintiffs' and the other Class
23 members' Personal Information to set up Third Party Service accounts and for payment, marketing,
24 and other purposes.

25 54. On April 1, 2011, SCEA transferred its online PSN and Qriocity service operations to
26 SNEA, including transferring Plaintiffs' and the other Class members' Personal Information to
27 SNEA for handling.

28

1 55. As part of that transfer, Sony required all PSN and Qriocity users to agree to a new
 2 Terms of Service and User Agreement (“New Agreement”) in order to continue using PSN and
 3 Qriocity. <http://www.qriocity.com/psnlegal/us/tos.html> (last visited May 3, 2011).

4 56. The New Agreement states, in pertinent part, that SNEA collects various data,
 5 including Personal Information and usage Data from PSN and Qriocity users as part of their use of
 6 Equipment and the PSN and Qriocity services. The New Agreement further states that such data is
 7 subject to the terms of SNEA’s Privacy Policy.

8 57. SNEA’s Privacy Policy applies to all visitors and users of PSN and Qriocity services,
 9 including Plaintiffs and the other members of the Class. It further states:

[SNEA] strive[s] to take reasonable measures to protect the confidentiality, security,
 and integrity of the personal information collected from our website visitors. Personal information is stored in secure operating environments that are not available to the public and that are only accessible to authorized employees. In addition, Sony Online Services use industry-standard encryption to prevent unauthorized electronic access to sensitive financial information such as your credit card number. We also have security measures in place to protect the loss, misuse, and alteration of the information under our control. . . . In the event of a security breach, we have procedures in place to protect our consumers’ data.

15 <http://www.qriocity.com/psnlegal/us/privacy.html> (last visited May 3, 2011).

16 58. SNEA’s Privacy Policy also states that SNEA may share Personal Information and
 17 usage Data with SCEA and that such shared content will also be protected according to SCEA’s
 18 Privacy Policy.

19 59. SCEA’s Privacy Policy states, in pertinent part,

[SCEA] take[s] reasonable measures to protect the confidentiality, security, and integrity of the personal information collected from our website visitors. Personal information is stored in secure operating environments that are not available to the public and that are only accessible to authorized employees. We also have security measures in place to protect the loss, misuse, and alteration of the information under our control.

23 <http://us.playstation.com/support/privacypolicy/index.htm> (last visited May 3, 2011).

24 60. SOE LLC has a similar Privacy Policy that applies to all users of SOE services. It
 25 states:

In order to provide you with added protection, SOE employs a security technology known as a secure-socket-layer (“SSL”) to protect the transmission of payment information to the Site. Unless otherwise specified herein or on the Site where you make a purchase, credit card numbers are used only for payment processing and are

1 not retained for marketing purposes. ... [W]e have in place reasonable technical and
2 organizational security measures to protect your Personal Information against
3 accidental or intentional manipulation, loss, destruction, or against unauthorized
4 disclosure or access to the information we collect online.

5 <http://www.soe.com/sonyonline/privacy.vm> (last visited May 3, 2011).

6 61. While these policies admonish that “there is no such thing as perfect security” they
7 plainly also state that Sony seeks to maintain or strives to take “reasonable security measures” and
8 other “reasonable measures to protect” Plaintiffs’ and the Class members’ Personal Information.

9 62. On information and belief, providing industry-standard security measures would
10 require Sony to spend a significant amount of money. However, by failing to provide industry-
11 standard security measures, Sony can save itself money, at least in the short term, at the cost of
12 increased risk to Sony’s customers from data or security breaches.

13 63. As with the situation of any other merchant who collects credit card or debit card
14 financial information from its customers, there is a reasonable expectation, independent of any
15 assurances provided in the policies quoted above, by Plaintiffs and the other Class members that
16 Sony would reasonably and adequately protect their financial information from use for any purpose
17 other than that to which it was intended by Plaintiffs and the other Class members, and certainly that
18 Sony would take reasonable and industry standard measures to protect that financial information
19 from theft.

20 64. As demonstrated more fully below, Sony failed to provide reasonable security
21 measures, failed to strive to maintain security, and otherwise maintained its Network in an unfair
22 manner, subjecting Plaintiffs and the other Class members to the concealed and unnecessary risk that
23 their Personal Information, which was made more vulnerable to data and security breaches than it
24 otherwise would have been had Sony behaved as it had promised and as is reasonably expected from
25 any merchant, and which was, in fact, compromised as a result.

26 **B. The Data Breach and Sony’s Failure to Disclose**

27 65. On information and belief, during the period April 16-17, 2011, a group of hackers
28 carried out a cyber-attack on Sony’s Network. During this attack, the hackers accessed and stole the

1 Personal Information of millions of Sony customers, including Plaintiffs and the other Class
2 members.

3 66. Sony knew or should have known that its Network was not secure and left Plaintiffs'
4 and the other Class members' Personal Information vulnerable to attack, theft, and misuse.

5 67. Sony recklessly, or as a matter of gross negligence, failed to provide reasonable and
6 adequate security measures—even when earlier threatened with an imminent attack.

7 68. Upon learning of the Data Breach, Sony failed to notify Plaintiffs and the other Class
8 members in a timely manner as required by law.

9 69. On or about April 16, 2011, Sony customers noticed intermittent interruptions to the
10 PSN. Unbeknownst to them, the outages were caused by the massive Data Breach. The Data Breach
11 would not have occurred if Sony properly had maintained, consistent with accepted industry
12 standards, adequate security measures designed to prevent unauthorized access to Plaintiffs' and the
13 other Class members' Personal Information stored on the Network.

14 70. On or about April 17, 2011, Sony discovered that PSN and Qriocity user data had
15 been compromised. Sony did not announce its discovery at the time.

16 71. Three days later, on April 20, 2011, Sony took the PSN and Qriocity offline. Sony
17 did not reveal the truth or the severity of the situation or the reasons for the shutdown to Plaintiffs
18 and the other Class members but, instead, simply advised them that “[w]e’re aware certain functions
19 of PlayStation Network are down. We will report back here as soon as we can with more
20 information.”¹ Sony’s advisory did not mention that a major security data breach had occurred, nor
21 did it inform Plaintiffs and the other Class members that their Personal Information had been
22 compromised or stolen.

23 72. By taking the PSN and Qriocity off-line, Sony denied Plaintiffs and the other Class
24 members access to their accounts, as well as to products and services only available through the PSN
25

26
27 ¹ See <http://blog.us.playstation.com/2011/04/20/update-on-psn-service-outages-2/>,
PLAYSTATION BLOG (last visited Dec. 10, 2012).

1 and Qriocity for which they had paid Sony and Third-Party Service providers valuable monetary
2 consideration.

3 73. On April 21, 2011, while the PSN and Qriocity remained off-line, Sony persisted in
4 its failure to tell the truth about the Data Breach to Plaintiffs and the other Class members.

5 74. Specifically, in a post to Sony's official on-line blog, Patrick Seybold, Sony's Senior
6 Director of Corporate Communications, stated:

7 While we are investigating the cause of the Network outage, we wanted to alert you
8 that it may be a full day or two before we're able to get the service completely back
9 up and running. Thank you very much for your patience while we work to resolve
this matter. Please stay tuned to this space for more details, and we'll update you
again as soon as we can.²

10 Again, Sony's public disclosures did not inform Plaintiffs and the other Class Members of the Data
11 Breach or that their Personal Information had been compromised or stolen.

12 75. On April 22, 2011, Sony continued to mislead and misinform Plaintiffs and the other
13 Class members about the cause of and reasons for the "Network outage," the occurrence of the Data
14 Breach, and the attendant damages and risks arising therefrom. Specifically, in another post to
15 Sony's official online blog, Mr. Seybold stated:

16 An external intrusion on our system has affected our PlayStation Network and
17 Qriocity services. In order to conduct a thorough investigation and to verify the
smooth and secure operation of our network services going forward, we turned off
18 PlayStation Network & Qriocity services on the evening of Wednesday, April 20th.
Providing quality entertainment services to our customers and partners is our utmost
19 priority. We are doing all we can to resolve this situation quickly, and we once again
thank you for your patience. We will continue to update you promptly as we have
20 additional information to share.³

21 76. Thus, despite possessing actual knowledge of the Data Breach, the severity thereof,
22 and the damages and risks posed to Plaintiffs and the other Class members, Sony elected to hide
23 these important facts about the massive security breach that had compromised the Personal
24 Information of over 77 million of its customers.

25 ² See <http://blog.us.playstation.com/2011/04/21/latest-update-on-psn-outage/>, PLAYSTATION
26 BLOG (last visited Dec. 10, 2012).

27 ³ See [http://blog.us.playstation.com/2011/04/22/update-on-playstation-network-qriocity-](http://blog.us.playstation.com/2011/04/22/update-on-playstation-network-qriocity-services/)
28 [services/](http://blog.us.playstation.com/2011/04/22/update-on-playstation-network-qriocity-services/), PLAYSTATION BLOG (last visited Dec. 10, 2012).

1 77. On April 25, 2011, six days after learning of the Data Breach and shutting down the
2 PSN, Sony again failed to inform Plaintiffs and the other Class members about what had occurred.
3 Specifically, in yet another post to its official on-line blog, Mr. Seybold stated:

4 I know you are waiting for additional information on when PlayStation Network and
5 Qriocity services will be online. Unfortunately, I don't have an update or timeframe
to share at this point in time.

6 As we previously noted, this is a time intensive process and we're working to get
7 them back online quickly. We'll keep you updated with information as it becomes
available. We once again thank you for your patience.⁴

8 Again, no word from Sony about the Data Breach or that Plaintiffs' and the other Class members'
9 Personal Information had been compromised or stolen.

10 78. Sony did not inform Plaintiffs and the other Class members of the Data Breach or the
11 damages and risks caused by the Data Breach until a full week after Sony learned of it. Specifically,
12 on April 26, 2011, Sony finally issued the following statement:

13 Although we are still investigating the details of this incident, we believe that an
14 unauthorized person has obtained the following information that you provided: name,
15 address (city, state, zip), country, email address, birthdate, PlayStation
16 Network/Qriocity password and login, and handle/PSN online ID. It is also possible
17 that your profile data, including purchase history and billing address (city, state, zip),
18 and your PlayStation Network/Qriocity password security answers may have been
obtained. If you have authorized a sub-account for your dependent, the same data
with respect to your dependent may have been obtained. While there is no evidence
at this time that credit card data was taken, we cannot rule out the possibility. If you
have provided your credit card data through PlayStation Network or Qriocity, out of
an abundance of caution we are advising you that your credit card number (excluding
security code) and expiration date may have been obtained.⁵

19 In conjunction with its belated disclosure, Sony put the burden on Plaintiffs and the other Class
20 members to monitor for damages caused by the Data Breach, cautioning them to watch out for
21 unauthorized use of their credit card data and identity-theft scams. Implicitly recognizing the damage
22

23
24
25 ⁴ See <http://blog.us.playstation.com/2011/04/25/psn-update/>, PLAYSTATION BLOG (last visited
26 Dec. 10, 2012).

27 ⁵ See <http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/>,
28 PLAYSTATION BLOG (last visited Dec. 10, 2012).

caused by the Data Breach, Sony encouraged Plaintiffs and the other Class members to “remain vigilant, to review your account statements and to monitor your credit reports.”⁶

79. Shortly after this “disclosure,” Sony admitted that its failure to protect Plaintiffs’ and the other Class members’ Personal Information gave rise to additional damage. Specifically, in posting answers to “Frequently Asked Questions,” Sony included the following questions and answers:

11. I want my money back (subscription fee, content) since the PSN/Qriocity was not available.

While we are still assessing the impact of this incident, we recognize that this may have had financial impact on our loyal customers. We are currently reviewing options and will update you when the service is restored.

12. There seems to be some games that cannot be played even offline?

Some games may require access to PSN for trophy sync, security checks or other network functionality and therefore cannot be played offline.

80. At the same time, Sony downplayed a brief interruption in SOE services. Specifically, Sony’s answers to “Frequently Asked Questions” regarding the Data Breach included the following question and answer:

8. Did SOE experience an attack due to the same reason?

SOE’s services are currently available, but they did experience a service interruption due to an external attack. An investigation is ongoing.⁷

81. On or around April 27, 2011, Sony explained that, with respect to SOE’s multiplayer online games, no data was compromised. Specifically, SOE LLC represented that it was “conducting a thorough investigation and, to the best of our knowledge, no customer personal information got out to any unauthorized person or persons.”⁸

⁶ *Id.*

⁷ See *Hackers stole personal data from PlayStation Network*, <http://ingame.msnbc.msn.com/news/2011/04/26/6538683-hackers-stole-personal-data-from-playstation-network>, MSNBC.COM (last visited Dec. 10, 2012).

⁸ See http://forums.station.sony.com/dcuops3/posts/list.m?topic_id=22096, SONY.COM (last visited Dec. 10, 2012).

82. On the morning of May 2, 2011, Sony took SOE off-line and advised Plaintiffs and the other Class members that the action was in response to “an issue that warrants enough concern for us to take the service down immediately.”⁹

83. Later that same day, Sony provided additional details. Specifically, in a Customer Service Notification posted on SOE’s web site, Sony disclosed – for the first time – that the names, addresses, e-mail addresses, gender, birthdates, phone numbers, log-in names, and hashed passwords of 24.6 million users registered on SOE had been compromised on or around April 16, 2011.¹⁰

84. On information and belief, the SOE data breach was carried out at the same time, and as part of, the PSN and Qriocity Data Breach.

85. On April 30, 2011, Sony announced that it would offer PSN and Qriocity users in the United States free identity theft protection service, certain free downloads and online services, and “will consider” helping customers who have to be issued new credit cards.¹¹

86. On May 12, 2011, Sony announced that it would offer SOE users in the United States free identity theft protection, one month of free service, and certain free in-game bonuses and currency.

87. Sony’s attempts to compensate its PSN, Qriocity, and SOE customers for damages arising from the Data Breach are grossly inadequate and were only made available to Sony customers for a limited and inadequate period of time.

C. Sony Knew or Should Have Known That Its Network Was Vulnerable to Attack

88. Sony knew or should have known that its unfair, unreasonable, and less than industry-standard security systems and technologies would leave its Network vulnerable to attacks by third-

⁹ See *Sony Online Entertainment servers shut down due to ‘issue’*, <http://ingame.msnbc.msn.com/news/2011/05/02/6570322-sony-online-entertainment-servers-shut-down-due-to-issue>, MSNBC.COM (last visited Dec. 10, 2012).

¹⁰ See *Sony Confirms Thousands of Credit Cards Stolen During Hack*, <http://www.gameinformer.com/b/news/archive/2011/05/02/thousands-of-credit-cards-stolen-during-second-sony-hack.aspx>, GAMEINFORMER.COM (last visited Dec. 10, 2012).

¹¹ See *Sony to restore PSN services, compensate customers*, http://news.cnet.com/8301-31021_3-20058731-260.html?tag=mncol;txt, CNET.COM (last visited Dec. 10, 2012).

1 parties. Sony, however, failed to take corrective measures to update its systems and technologies,
 2 even after Sony learned of prior security breaches and received a direct threat by a well-known
 3 group of hackers to infiltrate its Network.

4 89. Sony's Network had been compromised by unauthorized users a number of times
 5 before the massive April 2011 Data Breach. For example, in May 2009, reports surfaced that
 6 unauthorized copies of Sony's customers' credit cards were emailed to an outside account. And, in
 7 January 2011, hackers made the PlayStation game *Modern Warfare 2* unplayable through the PSN.

8 90. Upon information and belief, Sony was not taken by surprise when the Network was
 9 breached in April 2011, because Sony knew it had been breached on several prior occasions.

10 91. Similarly, in late 2010 and early 2011, a 19-year old man named George Hotz also
 11 successfully "jailbroke" the PS3 console and created an "exploit"—software or data that takes
 12 advantage of a vulnerability in a network to compromise the network and gain control of the system.
 13 Hotz's exploit allowed him to modify the PS3 console and use it with other operating systems, like
 14 Linux, to play "homebrewed" games. Such modification is relatively common among high-tech
 15 gamers, and other console manufacturers, such as Microsoft, silently have acquiesced to the practice.
 16 Indeed, earlier versions of the PlayStation console allowed users to modify them without resorting to
 17 such jailbreaks.¹²

18 92. Hotz publicly disclosed his exploit and Sony subsequently sued him for copyright
 19 infringement. In response to Sony's lawsuit against Hotz, the hacker collective known as
 20 "Anonymous" announced its outrage with Sony and publicly stated that it planned to attack the
 21 PSN.¹³

22 93. Just two weeks prior to the Data Breach, Anonymous sent the following message to
 23 Sony:

24 _____

25 ¹² See http://en.wikipedia.org/wiki/George_Hotz (last visited Dec. 10, 2012).

26 ¹³ See <http://anonops.blogspot.com/2011/04/opsony.html> (Apr. 3, 2011) (last visited Jan. 31,
 27 2012); see also *Anonymous calls out Sony over its treatment of hacker geohot*,
<http://www.theinquirer.net/inquirer/news/2040139/anonymous-calls-sony-treatment-hacker-geohot>,
 INQUIRER.NET (Apr. 4, 2011) (last visited Dec. 10, 2012).

1 You have abused the judicial system in an attempt to censor information on how your
 2 products work . . . Now you will experience the wrath of Anonymous. You saw a
 3 hornet's nest and stuck your [expletive] in it. You must face the consequences of
 4 your actions, Anonymous style . . . ***Expect us*** (emphasis added).¹⁴

5 94. Despite this direct threat to imminently breach the Network, Sony unreasonably and
 6 unfairly failed to implement adequate safeguards to protect its Network, including failing to take
 7 steps to protect Plaintiffs' and the other Class members' Personal Information stored on its Network.

8 95. Just two weeks before the April 2011 Data Breach, Sony laid off a substantial
 9 percentage of its Sony Online Entertainment workforce, including a number of employees in the
 10 Network Operations Center, which, according to Confidential Witness 2, is the group that is
 11 responsible for preparing for and responding to security breaches, and who ostensibly has the skills
 12 to bring the Network's security technology up-to-date.

13 96. During a press conference on May 1, 2011, Sony Corporation Chief Information
 14 Officer Shinji Hasejima admitted that Sony's Network was not secure at the time of the Date Breach,
 15 stating the attack was a "known vulnerability."¹⁵

16 **D. Sony Failed to Implement Basic Security Measures that Would Have Prevented**
 17 **the Massive April 2011 Data Breach**

18 97. On information and belief, Sony had not implemented reasonable, industry-standard,
 19 or appropriate security measures and knowingly, recklessly, or as a matter of gross negligence left
 20 Plaintiffs' and the other Class members' Personal Information stored on its Network vulnerable to
 21 one of the largest cyber-attacks and data thefts in history.

22 98. Despite Sony's duty to take reasonable steps to secure its Network, it in fact failed to
 23 take reasonable and adequate measures to protect Plaintiffs' and the other Class members' Personal
 24 Information stored on its Network.

25 ¹⁴ *See Id.*

26 ¹⁵ *See Sony's Kaz Hirai addresses PlayStation Network hack*, ENGADGET.COM,
 27 <http://www.engadget.com/2011/05/01/sonys-kaz-hirai-will-address-playstation-network-hack-at-lam-et/>
 28 (last visited Dec. 10, 2012).

1 99. On information and belief, among Sony's failures in this respect were its failure to
2 maintain adequate backups and/or redundant systems; failure to encrypt data and establish adequate
3 firewalls to handle a server intrusion contingency; failure to provide prompt and adequate warnings
4 of security breaches; and its unreasonable delay in bringing Sony Online Services back online after
5 the massive Data Breach.

6 100. As a leader in the computer technology industry, Sony had the ability and know-how
7 to implement and maintain sufficient online security consistent with industry standards.

8 101. According to Confidential Witness 1, Sony invested significant resources, including
9 firewalls, debug programs, and IP address limitations, to protect its own confidential proprietary
10 information housed on Sony's "development server," without incorporating the same safeguards on
11 the Network (such as a basic firewall). Access to the former could cause the *company* financial ruin,
12 while access to the latter could cause the financial ruin of *millions* of unsuspecting customers.

13 102. According to Confidential Witness 1, "Sony was more concerned about their
14 development server being hacked rather than some consumer's data being stolen. They want to
15 protect themselves and not the people that use their servers."

16 103. Sony's failure to install a firewall was confirmed by Confidential Witness 2, a
17 Platform Support Engineer for SOE LLC from 2006 until March 2011. According to this witness,
18 Sony's technicians only installed firewalls on an *ad-hoc* basis after they determined that a particular
19 user was attempting to gain unauthorized access to the Network.

20 104. On information and belief, while Sony implemented security systems and
21 technologies to protect its proprietary systems, it failed to employ its expertise as a technology leader
22 and other available expertise to implement similar security measures to protect Plaintiffs' and the
23 other Class members' Personal Information stored on its Network.

24 105. Sony's decision not to install and maintain appropriate firewalls on its Network
25 deviated from widespread industry practice and standards, including the Payment Card Industry Data
26
27
28

1 Security Standard (“PCI DSS”), which require anyone collecting payment card information to install
2 and maintain a firewall.¹⁶

3 106. Moreover, technology security experts at Attrition.org have stated that Sony’s lack of
4 encryption when storing Plaintiffs’ and the other Class members’ personal details and passwords was
5 both “reckless and ridiculous.” These experts went on to explain that “even security books from the
6 ‘80s were adamant about encrypting passwords at the very least.”¹⁷

7 107. According to Confidential Witness 3, a former Quality Assurance Analyst with SOE
8 LLC from January 2010 to March 2011, SCEA, the division responsible for the PS3 console and
9 Network, was not nearly as secure as SOE.

10 108. The PS3 console itself may also unnecessarily compromise data security.
11 Confidential Witness 4 explained that PS3 consoles are supposed to be secured by a “random
12 number generator,” but are not. Indeed, each console has the same access number – rendering the
13 PS3 particularly susceptible to security breaches since access to one provides access to all.

14 109. On June 8, 2011, Sony’s Deputy President, admitted that, at the time of the Data
15 Breach, Sony’s Network failed to meet minimum security standards. When asked whether Sony had
16 revised its security systems following the April 2011 Data Breach, Mr. Hirai stated that Sony has
17 “done everything to bring our practices at least in line with industry standards or better.”¹⁸

18 **E. Industry Experts, Academics, and United States Senators Have Criticized Sony**
19 **for Failing to Protect the Personal Information of Its Customers**

20 110. In response to the massive April 2011 Data Breach, Sony has represented that it
21 implemented basic measures to defend against new attacks, including the following systems that

22
23 ¹⁶ The PCI DSS “is an information security standard for organizations that handle cardholder
24 information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.”
http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard (last visited Dec. 10,
2012).

25 ¹⁷ See *Absolute Sownage: A concise history of recent Sony hacks*, ATTRITION.ORG (June 4,
26 2011), http://attrition.org/security/rant/sony_aka_sownage.html (last visited Dec. 10, 2012).

27 ¹⁸ See *E3 2011: Sony’s Kaz Hirai on the PSN hack*, GUARDIAN.CO.UK (June 8, 2011),
<http://www.guardian.co.uk/technology/2011/jun/08/e3-2011-sony-psn> (last visited Dec. 10, 2012).

1 should have been in place prior to April 2011: automated software monitoring; enhanced data
 2 encryption; enhanced ability to detect intrusions to the Network, such as an early-warning system to
 3 detect unusual activity patterns; and additional firewalls. Additionally, Sony hired a Chief
 4 Information Security Officer.¹⁹

5 111. Had Sony been acting fairly and reasonably toward Plaintiffs and the Class, all of
 6 these new measures would have been in place before the Data Breach. But they were not. Indeed,
 7 Confidential Witness 4, a Product Service Manager at SCEA from January 2005 until March 2011,
 8 likened these measures to “getting an alarm system installed after you have been burglarized.”

9 112. John Bumgarner, Chief Technology Officer of the independent, non-profit research
 10 institute United States Cyber-Consequences Unit, found that as of May 10, 2011, the PSN was still
 11 vulnerable to attacks. Specifically, unauthorized users could still access internal Sony resources,
 12 including security-management tools. Indeed, Bumgarner’s research showed that the problems with
 13 Sony’s systems were more widespread than Sony had acknowledged at that time.²⁰

14 113. Mr. Bumgarner was correct and, as described below, the Sony Pictures Entertainment
 15 network was breached on June 2, 2011. LulzSec, the hacking collective that claimed responsibility
 16 for that incident, stated that its motivation was to show that Sony lied when it told customers that it
 17 had revamped security to protect against the same type of attack that occurred in April 2011.²¹

21 ¹⁹ See *Sony Battens Down the Hatches for PlayStation Network, Hiring CISO*,
 22 SECURITYWEEK.COM (May 2, 2011), [http://www.securityweek.com/sony-battens-down-hatches-](http://www.securityweek.com/sony-battens-down-hatches-playstation-network-hiring-ciso)
 23 [playstation-network-hiring-ciso](http://www.securityweek.com/sony-battens-down-hatches-playstation-network-hiring-ciso) (last visited Dec. 10, 2012); *Sony recruits information security boss*
after hacking, REUTERS.COM (Sept. 6, 2011), [http://www.reuters.com/article/2011/09/06/us-sony-](http://www.reuters.com/article/2011/09/06/us-sony-idUSTRE7851PH20110906)
[idUSTRE7851PH20110906](http://www.reuters.com/article/2011/09/06/us-sony-idUSTRE7851PH20110906) (last visited Dec. 10, 2012).

24 ²⁰ See *Sony yet to fully secure its networks: expert*, REUTERS.COM (May 13, 2011),
 25 <http://www.reuters.com/article/2011/05/13/us-sony-idUSTRE74C70420110513> (last visited Dec. 10,
 2012).

26 ²¹ See *Sony Pictures falls victim to major data breach*, COMPUTERWORLD.COM (June 2, 2011),
 27 http://www.computerworld.com/s/article/9217273/SonyPictures_falls_victim_to_major_data_breach
 (last visited Dec. 10, 2012).

114. Indeed, numerous experts in the field attribute the Sony Pictures data breach to an unsophisticated method of hacking that would not have been successful if Sony had even the most basic security measures in place.

115. For example, Tony Bradley, a *PCWorld* journalist who covers technology issues, in a June 3, 2011 article entitled, “Sony Hacked Again: How Not To Do Network Security,” stated that Sony “seems to ignore compliance requirements and basic security best practices, so it is basically begging to be attacked.”²² Bradley further advised that companies should follow security “best practices and data security compliance requirements”—and in short—“[d]on’t be a Sony.”²³

116. Similarly, according to Fred Touchette of AppRiver, an email and web security software provider: “[t]here is no doubt that Sony needs to spend some major effort in tightening up its network security. This latest hack against them was a series of simple SQL Injection attacks against its web servers. This simply should not have happened.”²⁴

117. Sony’s delay in publicly disclosing the Data Breach sparked concern and outrage, causing U.S. Senator Richard Blumenthal (D-Conn.) to condemn Sony’s lack of reasonable security measures, stating that: “Sony persists in unconscionably refusing to alert its millions of users on the PlayStation Network proactively, while they remain at serious risk of identity theft and other financial attacks stemming from their personal and financial data having been compromised.”²⁵

118. Sony customers similarly have expressed their unhappiness and dissatisfaction with Sony’s conduct, including the editors of the gamer website IGN.com:

(a) Hilary: “[I]t’s disheartening to see a company respond so poorly to the biggest crisis it’s faced this console generation . . . Faced with a crisis that

²² See Tony Bradley, *Sony Hacked Again: How Not to Do Network Security*, PCWORLD.COM (June 3, 2011), http://www.pcworld.com/businesscenter/article/229351/sony_hacked_again_how_not_to_do_network_security.html (last visited Dec. 10, 2012).

²³ *Id.*

²⁴ *Id.*

²⁵ See Press Release, Blumenthal Continues to Push Sony over Playstation Data Breach (Apr. 27, 2011), <http://blumenthal.senate.gov/newsroom/press/release/blumenthal-continues-to-push-sony-over-playstation-data-breach> (last visited Dec. 10, 2012).

1 affected its customers, people at Sony ignored compassion, eschewed
 2 openness and instead hid in silence . . . While your credit card info may have
 3 been exposed to criminals that brought down Sony's service, leaving those
 4 loyal to PlayStation in potential financial peril, executives chose to keep their
 mouths shut . . . Their true selves were revealed – as selfish, greedy, self-
 centered individuals more concerned with the bottom line than the value of
 their customer base.”

5 (b) Charles: “It shouldn’t have taken this long for Sony to issue a statement
 6 about this kind of thing. Customer security should be the number one priority
 if Sony wants its consumer base to maintain faith in its service.”

7 (c) Tom: “[F]or Sony to wait 6 whole days before holding their hands up to
 8 admit 75 million people’s PSN details - including credit card details - could
 have been compromised, is galling to say the least.”²⁶

9 **F. The Data Breach, Caused by Sony’s Improper Conduct, Has Harmed Plaintiffs**
 10 **and the Other Class Members**

11 **i. Identity Theft**

12 119. As a result of Sony’s unreasonable, unfair, inadequate, and less than industry standard
 13 security for the Network, cyber-criminals now possess the Personal Information of Plaintiffs and the
 14 other Class members. While credit card companies offer protection against unauthorized charges, the
 15 process is long, costly, and frustrating. Physical cards must be replaced, credit card information
 16 must be updated on all automatic payment accounts, and victims must add themselves to credit fraud
 17 watch lists, which substantially impairs victims’ ability to obtain additional credit. Immediate notice
 18 of the breach is essential to obtain the best protection afforded by these services. As alleged above,
 19 Sony failed to provide such immediate notice, thus further exacerbating the damages sustained by
 20 Plaintiffs and the other Class members arising from the Data Breach.

21 120. Companies recognize that Personal Information is a valuable asset, and Symantec
 22 Corporation has even created a software application that values a person’s identity on the black
 23 market.²⁷

25 ²⁶ See *The Lobby: PlayStation Network Down*, *The IGN Editors weigh in on the disastrous*
 26 *breach of the PlayStation Network*, IGN.com (Apr. 26, 2011), <http://m.ign.com/articles/1164195>
 (last visited Dec. 10, 2012).

27 ²⁷ See Risk Assessment Tool, Norton 2010, [http://www.everyclickmatters.com/victim/assessment-](http://www.everyclickmatters.com/victim/assessment-tool.html)
 28 [tool.html](http://www.everyclickmatters.com/victim/assessment-tool.html); see also T. Soma, *et al*, *Corporate Privacy Trend: The “Value” of Personally Identifiable*

121. Personal Information is a valuable commodity. A “cyber black-market” exists in which criminals openly post stolen credit card numbers, Social Security numbers, and other personally identifiable information on a number of Internet websites. As one industry report recognized, this “credit card black-market operates very much in the open” and a number of websites exist that offer stolen credit card numbers and associated credentials. The report went on to state:

It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it’s very “in your face.”

<http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/> (last accessed on December 10, 2012).

ii. Cyber-stalking and Spam

122. Information about Plaintiffs and the other Class Members may also be used to harass or stalk them. And, the threat of “spear phishing”—where details of a person’s Usage Data can be used to tailor a “phishing” message that looks authentic, but is actually a ruse to get the consumer to divulge account information—is real.

123. Indeed, at the time it disclosed the Data Breach, Sony cautioned its customers that the breach might lead to email, telephone, and postal scams that ask for personal information.

iii. Lost Use of Sony Online Services

124. PSN and Qriocity remained offline for almost a month while Sony conducted an audit of its systems to determine exactly how the Data Breach occurred. Similarly, SOE remained offline for more than two weeks. During this prolonged period of downtime, Plaintiffs and the other Class members were unable to access PSN, Qriocity, and SOE; purchase “add-ons” with their virtual wallets; access “add-ons” or other Downloads they had already purchased; play multi-player online games with others; and to otherwise use online services available through the PSN, Qriocity, and

Information (“PII”) Equals the “Value” of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009).

1 SOE. Plaintiffs and the other Class members were also unable to access and use prepaid Third-Party
2 Services, such as Netflix, MLB.TV, and NHL Gamecenter Live.

3 125. As CNET News explained, the harm caused by the Data Breach and Sony's
4 associated shut down of its PSN as a result thereof was real and expansive:

5 While it's free to sign up for PlayStation Network, much of the content that can be
6 downloaded requires a separate subscription to use, and every day that customers
7 can't access that content, they're essentially losing money for something they've
8 prepaid for. And it's not just games.

9 Other examples include [1] the Netflix app that can be downloaded from the PSN
10 Store and used to access Netflix's Watch Instantly subscription feature; [2]
11 MLB.TV's \$100-per-season game package, which lets users watch MLB games on a
12 TV via the PS3; [3] the paid version of Hulu, Hulu Plus and more.

13 PSN Plus customers are also losing money, since they pay for year or several months
14 blocks of time to access exclusive content from PSN. As of now, they are also unable
15 to play some games they've already downloaded because PSN has to be operational
16 to play.²⁸

17 126. For Plaintiffs and the other Class members, the lost use of pre-paid services
18 significantly lessened the value of their PS3s and PSPs, which they purchased with the expectation
19 that the Network would be reasonably accessible for services like online gaming, store purchases,
20 game downloads, and Third-Party Services, such as Netflix.

21 127. As alleged above, four of Plaintiffs paid a monthly fee for the Third-Party Service
22 Netflix to use through their PS3s but, due to the Data Breach and concomitant PSN outage, were
23 unable to use Netflix through their PS3s.

24 **iv. Sony Admits that It Harmed Plaintiffs and the Other Class Members**

25 128. During a press conference on Sunday, May 1, 2011, the Chairman of Sony Computer
26 Entertainment, Kazuo Hirai, readily acknowledged that Sony's failure to protect its customers'
27 Personal Information had harmed its customers:

28 Again we like to offer our deepest and sincere apologies for potentially
compromising customer data as well as causing great concern and making services
unavailable for an extended period of time.

²⁸ See *Five questions for Sony about PSN breach*, CNET.COM (Apr. 27, 2011),
http://news.cnet.com/8301-31021_3-20057963-260.html (last visited Dec. 10, 2012).

G. Since the April 2011 Data Breach, Sony has Experienced Numerous Other Security Breaches that Call Into Question its Ability to Safeguard its Customers' Personal Information Against Future Attacks

129. On May 18, 2011, just four days after restoring the PSN, Sony took down certain websites that allow PSN users to sign in and restore their passwords. According to Sony, it had discovered, and subsequently fixed, a URL exploit that allowed hackers to change user passwords with the Personal Information stolen during the April 2011 Data Breach.

130. On June 2, 2011, LulzSec announced that it had broken into Sony Pictures Entertainment servers and compromised the personal information of over 1 million individuals, including the names, email addresses, home addresses, telephone numbers, gender, website passwords, user names, dates of birth, associated with their accounts.

131. According to LulzSec, it was able to access and obtain this personal information by using an elementary hacking device known as an "SQL Injection," which it described as "one of the most primitive and common vulnerabilities." The group further claimed that from a "single injection" it "accessed EVERYTHING," and that it was able to do so "easily" and "without the need for outside support or money."²⁹

132. Even more damning, LulzSec claimed that the data it stole was not encrypted or hidden behind a cryptographic hash tag, but flagrantly stored in plain text.³⁰ LulzSec also posted on its website certain hijacked Personal Information, including email addresses and passwords, of thousands of Sony customers.³¹

133. Most recently, on October 12, 2011, Sony disclosed that between October 7, 2011 and October 10, 2011, intruders staged a massive attempt to access user accounts on the PSN and other

²⁹ See *Sony Pictures website hacked, 1 million accounts compromised*, BGR.COM (June 2, 2011), <http://www.bgr.com/2011/06/02/sony-pictures-website-hacked-1-million-accounts-compromised/> (last visited Dec. 10, 2012) (emphasis in original).

³⁰ See *Sony LulzSec Hack: What You Need to Know*, PCMAG.COM (June 3, 2011), <http://www.pcmag.com/article2/0,2817,2386362,00.asp> (last visited Dec. 10, 2012).

³¹ *Id.*

1 online entertainment services. In response, Sony locked approximately 93,000 user accounts whose
 2 identities and passwords were successfully obtained during the October 2011 intrusion.³²

3 **CLASS ACTION ALLEGATIONS**

4 134. Plaintiffs bring this lawsuit on behalf of themselves and as a class action, pursuant to
 5 Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure, on behalf of a proposed class (the
 6 “Class”), defined as:

7 All persons and entities in the United States that subscribed to the PlayStation
 8 Network, Qriocity and/or Sony Online Entertainment prior to April 16, 2011.

9 135. Excluded from the Class are Defendants, including any entity in which Defendants
 10 have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as
 11 the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of
 12 Defendants.

13 136. Plaintiffs also seek certification of individual state subclasses for California, Florida,
 14 Massachusetts, Michigan, Missouri, New Hampshire, New York, Ohio, and Texas (collectively,
 15 State Subclasses”) pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure,
 16 defined as:

17 All persons and entities in [Subclass State] that subscribed to the PlayStation
 18 Network, Qriocity and/or Sony Online Entertainment service prior to April 16, 2011.

19 137. Excluded from the State Subclasses are Defendants, including any entity in which
 20 Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by
 21 Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors,
 22 successors, and assigns of Defendants.

23 138. Certification of Plaintiffs’ claims for class-wide treatment is appropriate because
 24 Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as
 25 would be used to prove those elements in individual actions alleging the same claims.

26 ³² See *Sony PlayStation Network Hacked Again, Closes 93,000 Accounts*, ABCNEWS.GO.COM
 27 (Oct. 12, 2011), <http://abcnews.go.com/blogs/technology/2011/10/sony-playstation-network-hacked-again-closes-93000-accounts/> (last visited Dec. 10, 2012).

1 139. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the Class
 2 are so numerous that joinder of all members would be impracticable. Upon information and belief,
 3 there were approximately 77 million PSN and Qriocity users worldwide impacted by the Data
 4 Breach. Approximately 31 million of those 77 million PSN and Qriocity users reside in the United
 5 States. In addition, on May 3, 2011, Sony issued a press release announcing that the “personal
 6 information from approximately 24.6 million SOE accounts may have been stolen.” While the exact
 7 number of Class members is currently unknown to Plaintiffs, upon information and belief, Plaintiffs
 8 allege that there are, at least, tens of millions of Class members who were damaged by Sony’s
 9 conduct described herein. The names and addresses of Class members are identifiable through
 10 documents maintained by Sony. Ultimately, the sheer number of Class members, who are
 11 geographically dispersed around the United States, makes joinder of all members impracticable.

12 140. **Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2) and**
 13 **23(b)(3).** This action involves common questions of law or fact, which predominate over any
 14 questions affecting individual Class members, including:

- 15 (a) whether Sony engaged in the wrongful conduct alleged herein;
- 16 (b) whether Sony owed a legal duty to Plaintiffs and the other Class members to
- 17 exercise due care in collecting, storing, and safeguarding their Personal Information;
- 18 (c) whether Sony breached legal duties owed to Plaintiffs and the other Class
- 19 members to exercise due care in collecting, storing, and safeguarding their Personal Information;
- 20 (d) whether Sony’s conduct violated the consumer protection laws of the states of
- 21 California, Florida, Massachusetts, Michigan, Missouri, New Hampshire, New York, Ohio, and
- 22 Texas;
- 23 (e) whether Sony has been unjustly enriched through its acts and/or omissions
- 24 alleged herein;
- 25 (f) whether Sony violated the Fair Credit Reporting Act by failing to adequately
- 26 secure Plaintiff’s and the other Class members’ Personal Information;
- 27 (g) whether Plaintiffs and the other Class members are entitled to actual,
- 28 statutory, or other forms of damages, and other monetary relief; and

1 (h) whether Plaintiffs and the other Class members are entitled to equitable relief,
2 including, but not limited to, injunctive relief and restitution.

3 141. Sony engaged in a common course of conduct giving rise to the legal rights sought to
4 be enforced by Plaintiffs individually and on behalf of the other Class members. Similar or identical
5 statutory and common law violations, business practices, and injuries are involved. Individual
6 questions, if any, pale by comparison, in both quality and quantity, to the numerous common
7 questions that dominate this action.

8 142. **Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are
9 typical of the claims of the other Class members because, among other things, Plaintiffs and the
10 other Class members were injured through the substantially uniform misconduct described above.
11 Plaintiffs herein are advancing the same claims and legal theories on behalf of themselves and all
12 other Class members, and there are no defenses available to Sony that are unique to Plaintiffs.

13 143. **Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4).**
14 Plaintiffs are adequate representatives of the Class because their interests do not conflict with the
15 interests of the other Class members they seek to represent; they have retained—and the Court has
16 appointed—counsel competent and experienced in complex class action litigation; and Plaintiffs will
17 prosecute this action vigorously. The Class' interests will be fairly and adequately protected by
18 Plaintiffs and their counsel.

19 144. **Superiority – Federal Rule of Civil Procedure 23(b)(3).** A class action is superior
20 to any other available means for the fair and efficient adjudication of this controversy, and no
21 unusual difficulties are likely to be encountered in the management of this matter as a class action.
22 The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other
23 Class members are relatively small compared to the burden and expense that would be required to
24 litigate their claims on an individual basis against Sony, making it impracticable for Class members
25 to individually seek redress for Sony's wrongful conduct. Even if Class members could afford
26 individual litigation, the court system could not. Individualized litigation would create a potential for
27 inconsistent or contradictory judgments, and increase the delay and expense to all parties and the
28 court system. By contrast, the class action device presents far fewer management difficulties and

1 provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a
2 single court.

3 145. This is particularly true here, because Sony's "Terms of Service and User
4 Agreement" mandates the application of California law to Plaintiffs' and the other Class members'
5 claims.

6 **CLAIMS ASSERTED**

7 **COUNT 1**

8 **Violation of California's Unfair Competition Law ("UCL")** 9 **Cal. Bus. & Prof. Code § 17200 *et seq.*** 10 **(On Behalf of California Plaintiffs Arthur Howe and Kyle Johnson** 11 **and the California Subclass)**

12 146. California Plaintiffs Arthur Howe and Kyle Johnson, individually and on behalf of
13 the other California Subclass members, repeat, reallege, and incorporate by reference the allegations
14 contained in paragraphs 1-145 above, as though fully stated herein.

15 147. Sony engaged in unfair, unlawful, and fraudulent business practices in violation of the
16 UCL.

17 148. By reason of the conduct alleged herein, Sony engaged in unlawful, unfair, and
18 deceptive practices within the meaning of the UCL. The conduct alleged herein is a "business
19 practice" within the meaning of the UCL.

20 149. Sony violated the UCL by failing to take reasonable precautions to protect California
21 Subclass members' Personal Information as alleged. Further, Sony promised to take "reasonable
22 measures" to protect customers' Personal Information against breaches in security, but failed to do
23 so. In violation of industry standards, Sony used weak or no encryption and failed to adequately
24 install and maintain firewalls, as alleged more fully in this complaint. Sony was aware of previous
25 attempts to break into its Network but failed to rectify shortcomings in its security systems and
26 technologies that allowed for those breaches and ensuing Data Breach to be successful. Sony
27 violated consumer expectations to safeguard Personal Information and failed to tell consumers that it
28 did not have reasonable and adequate safeguards in place to protect California Subclass members'
Personal Information.

1 150. Sony also violated the UCL by failing to immediately notify California Subclass
2 members of the Data Breach. If California Subclass members had been notified in an appropriate
3 fashion, they could have taken precautions to safeguard their Personal Information.

4 151. Sony misrepresented that access to the PSN was a feature of PS3s and PSPs. *See*
5 <http://us.playstation.com/ps3/features/ps3featuresnetwork.html> (last visited on Dec. 10, 2012).

6 152. Sony misrepresented that online connectivity and corresponding ability to connect to
7 Qriocity, SOE, and Third-Party Services, such as Netflix, was a feature of PS3s and PSPs. *See*
8 http://us.playstation.com/ps3/features/ps_ps3_connectivity.html (last visited on Dec. 10, 2012).

9 153. Sony's acts, omissions, and misrepresentations as alleged herein were unlawful and in
10 violation of, *inter alia*, Cal. Bus. & Prof. Code §17500 *et seq.*, Cal. Civ. Code §1750 *et seq.*, Cal.
11 Civ. Code § 1798.80 *et seq.*, and its own Privacy Policy.

12 154. Continued access to the PSN was a substantial factor in Plaintiff Howe's and Plaintiff
13 Johnson's purchases of their PS3s.

14 155. Sony's actions also constitute "unfair" business acts or practices because, as alleged
15 above, *inter alia*, Defendants omitted material facts regarding its Network, and thereby offended
16 public policy and engaged in immoral, unethical, oppressive, and unscrupulous activities that caused
17 substantial injury to consumers, including California Subclass members. The gravity of Sony's
18 conduct outweighs any potential benefits attributable to such conduct. And, there were reasonably
19 available alternatives to further Sony's legitimate business interests, other than Sony's conduct
20 described herein. Further, Sony has violated public policy, as expressed through laws and
21 regulations, to adopt reasonable procedures for meeting the needs of commerce for consumer credit,
22 personnel and other information in a manner which is fair and equitable to the consumer with regard
23 to confidentiality and proper utilization of such information, in violation of the unfair prong of the
24 UCL.

25 156. Sony's representations and other conduct induced Plaintiffs Howe and Johnson to
26 purchase PS3s, to purchase and/or register for Sony's Online Services, to provide Personal
27 Information when purchasing and/or registering for Sony's Online Services, and to purchase content
28 from the Network and the PlayStation Store. But for these deceptive acts and business practices,

1 Plaintiffs Howe and Johnson would not have purchased PS3s, or would not have paid the prices they
 2 paid for their PS3s, and would not have prepaid for Third-Party Services from or used through the
 3 Network.

4 157. Plaintiffs Howe and Johnson suffered injury in fact and lost money or property as the
 5 result of Sony's failure to secure their Personal Information that was stored on Sony's servers. As a
 6 result of the Data Breach, Plaintiff Howe's and Plaintiff Johnson's Personal Information was
 7 compromised, they lost the unencumbered use of their passwords, their passwords were obtained by
 8 a third party without their consent, and they lost the use of Sony Online Services. Additionally, other
 9 applications and products that can only be used through the Network were rendered worthless,
 10 because Plaintiff Howe and Plaintiff Johnson were unable to access said features due to Sony's
 11 disabling of its Network.

12 158. The value of and utility of Plaintiffs Howe and Johnson's and the other California
 13 Subclass members' PS3s and PSPs was diminished as the result of Sony's failure to secure their
 14 Personal Information and the corresponding taking down of Sony Online Services for an extended
 15 period of time.

16 159. California Subclass members would not have registered/subscribed to Sony Online
 17 Services or provided Sony with their Personal Information had they known of Sony's failure to
 18 maintain adequate or reasonable security measures to protect their Personal Information in its
 19 possession.

20 160. As a result of Sony's wrongful conduct, Plaintiffs Howe and Johnson and the other
 21 members of the California Subclass are entitled to restitutionary and injunctive relief.

22 COUNT 2

23 **Violation of California's False Advertising Law ("FAL")** 24 **Cal. Bus. & Prof. Code § 17500 *et seq.*** **(On Behalf of California Plaintiffs Arthur Howe and Kyle Johnson** 25 **and the California Subclass)**

26 161. California Plaintiffs Arthur Howe and Kyle Johnson, individually and on behalf of
 27 the other California Subclass members, repeat, reallege, and incorporate by reference the allegations
 28 contained in paragraphs 1-145 above, as though fully stated herein.

1 162. Sony engaged in deceptive and misleading advertising in violation of the FAL.

2 163. Sony violated the UCL by omitting that its Network was not sufficiently secure, by
3 promising to take “reasonable measures” to protect customers’ Personal Information against
4 breaches in security, but not doing so. In violation of industry standards, Sony used weak or no
5 encryption and failed to adequately install and maintain firewalls. Sony was aware of previous
6 attempts to break into its Network but failed to rectify shortcomings in its security systems and
7 technologies that allowed for those breaches and ensuing Data Breach to be successful.

8 164. Sony misrepresented that access to the PSN was a feature of PS3s and PSPs. *See*
9 <http://us.playstation.com/ps3/features/ps3featuresnetwork.html> (last visited on Dec. 10, 2012).

10 165. Sony omitted facts concerning and misrepresented that online connectivity and
11 corresponding ability to connect to Qriocity, SOE, and Third Parties Services, such as Netflix, was a
12 feature of PS3s and PSPs. *See* http://us.playstation.com/ps3/features/ps_ps3_connectivity.html (last
13 visited on Dec. 10, 2012).

14 166. Sony’s omissions, representations and other conduct induced Plaintiffs Howe and
15 Johnson to purchase PS3s, to purchase and/or register for Sony Online Services, and to provide
16 Personal Information when purchasing and/or registering for Sony Online Services or purchasing
17 content from the Network or the PlayStation Store. But for these deceptive acts and business
18 practices, Plaintiffs Howe and Johnson would not have purchased PS3s, or would not have paid the
19 prices they paid for their PS3s and/or PSPs, and/or would not have prepaid for Third-Party Services
20 from or used through the Network.

21 167. Continued access to the PSN was a substantial factor in Plaintiff Howe’s and Plaintiff
22 Johnson’s purchases of their PS3s.

23 168. Plaintiffs Howe and Johnson suffered injury in fact and lost money or property as the
24 result of Sony’s failure to secure their Personal Information that was stored on Sony’s Network. As
25 the result of the Data Breach, Plaintiff Howe’s and Plaintiff Johnson’s Personal Information was
26 compromised, they lost the unencumbered use of their passwords, their password was obtained by a
27 third party without their consent, and lost the use of Sony Online Services as the result of the Data
28 Breach. Additionally, other applications and products that can only be used through the Network

1 were rendered worthless, because they were unable to access said features due to Sony's disabling of
2 its Network.

3 169. The value of Plaintiff Howe's, Plaintiff Johnson's, and the other California Subclass
4 members PS3s and/or PSPs was diminished as the result of Sony's failure to secure their Personal
5 Information and corresponding taking down of the Network for an extended period of time.

6 170. California Subclass members would not have registered/subscribed to Sony Online
7 Services or provided Sony with their Personal Information had they known of Sony's failure to
8 maintain adequate or reasonable security measures to protect their Personal Information in its
9 possession.

10 171. As a result of Sony's violation of the FAL, California Subclass members are entitled
11 to an order enjoining Sony from continuing the deceptive advertising described herein. California
12 Subclass members are also entitled to restitution for the economic harm they have suffered as a
13 result of the diminution in value of their PS3s and/or PSPs and prepaying for access to certain
14 services on the PSN, Qriocity, SOE, and Third-Party Services, such as Netflix. California Subclass
15 members also suffered economic harm on account of purchasing PS3 games that were advertised and
16 promoted based on their extensive multiplayer features that are only accessible via the PSN, and the
17 value of which was substantially reduced because they were unable to access said features due to
18 Sony's disabling of the PSN.

19 **COUNT 3**

20 **Violation of California's Consumers Legal Remedies Act ("CLRA")** 21 **Cal. Civ. Code § 1750 *et seq.*** 22 **(On Behalf of California Plaintiffs Arthur Howe and Kyle Johnson** 23 **and the California Subclass)**

24 172. California Plaintiffs Arthur Howe and Kyle Johnson, individually and on behalf of
25 the other California Subclass members, repeat, reallege, and incorporate by reference the allegations
26 contained in paragraphs 1-145 above, as though fully stated herein.

27 173. The CLRA was enacted to protect consumers against unfair and deceptive business
28 practices. It extends to transactions that are intended to result, or which have resulted, in the sale or
lease of goods or services to consumers. Sony's acts, omissions, representations and practices as

described herein fall within the CLRA because the design, development, and marketing of Sony's Equipment and Network services are intended to and did result in sales of PS3s, PSPs, and Network services.

174. Plaintiffs Howe and Johnson and the other California Subclass members are consumers within the meaning of Cal. Civ. Code §1761(d).

175. Sony's acts, omissions, misrepresentations, and practices were and are likely to deceive consumers. By omitting key information about the safety and security of the Network and deceptively representing that it adequately maintained such information, Sony violated the CLRA. Sony had exclusive knowledge of undisclosed material facts, namely, that its Network was defective and/or unsecure, and withheld that knowledge from California Subclass members. Additionally, Sony misrepresented that a feature of PS3s and PSPs was access to the PSN.

176. Sony's acts, omissions, misrepresentations, and practices alleged herein violated the following provisions of the CLRA, which provides, in relevant part, that:

(a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful:

(5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have

(7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.

(9) Advertising goods or services with intent not to sell them as advertised.

(14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law.

(16) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

For purposes of the CLRA, omissions are actionable along with representations.

177. Sony stored California Subclass members' Personal Information on its Network. Sony represented to California Subclass members that its Network was secure and that their Personal Information would remain private. Sony engaged in deceptive acts and business practices by providing in its Privacy Policy that it uses "reasonable measures to protect the confidentiality,

1 security, and integrity of the personal information collected from [its] website visitors,” and that it
2 maintains security measures “to protect the loss, misuse, and alteration of the information under our
3 control.”

4 178. Sony knew or should have known that it did not employ reasonable measures that
5 would have kept California Subclass members’ Personal Information secure and prevented the loss
6 or misuse of their Personal Information. For example, Sony failed to use a sufficient encryption code
7 to protect California Subclass members’ financial information and failed to employ any encryption
8 to protect other personal information, such as email addresses and passwords.

9 179. Sony’s deceptive acts and business practices induced California Subclass members to
10 purchase PS3s and/or PSPs, to purchase or register for Sony Online Services, and to provide
11 Personal Information, including credit card information, for the purchase of content from the
12 Network or the PlayStation Store. But for these deceptive acts and business practices, California
13 Subclass members would not have purchased PS3s, PSPs and/or prepaid for Third-Party Services
14 from or used through the Network, or would not have paid the prices they paid for PS3s, PSPs,
15 and/or Third-Party Services from or used through the Network.

16 180. Sony’s representations that access to the PSN was a feature of PS3s and PSPs and
17 that it would secure and protect California Subclass members’ Personal Information in its possession
18 were facts that reasonable persons could be expected to rely upon when deciding whether to
19 purchase PS3s, PSPs, Sony Online Services, and/or Third-Party Services from or used through the
20 Network.

21 181. California Subclass members were harmed as the result of Sony’s violations of the
22 CLRA, because their Personal Information was compromised, placing them at a greater risk of
23 identity theft; they lost the unencumbered use of their password; and their passwords were disclosed
24 to third parties without their consent.

25 182. California Subclass members suffered injury in fact and lost money or property as the
26 result of Sony’s failure to secure their Personal Information; the values of their PS3s and/or PSPs
27 were diminished as the result of Sony’s failure to secure their Personal Information and
28 corresponding taking down of Sony Online Services for an extended period of time; and applications

1 and products that can only be accessed through the Network were rendered worthless, because
 2 California Subclass members were unable to access said features due to Sony's disabling of the
 3 Network.

4 183. Sony's conduct alleged herein was oppressive, fraudulent, and/or malicious, thereby
 5 justifying an award of punitive damages.

6 184. As the result of Sony's violation of the CLRA, California Subclass members are
 7 entitled to compensatory and exemplary damages, an order enjoining Sony from continuing the
 8 unlawful practices described herein, a declaration that Sony's conduct violated the CLRA, restitution
 9 as appropriate, attorneys' fees, and the costs of litigation.

10 185. Pursuant to Cal. Civ. Code §1782, on June 8, 2011, Plaintiff Johnson mailed Sony
 11 notice in writing, via U.S. certified mail, of the particular violations of Cal. Civ. Code §1770 of the
 12 CLRA and demanded that Sony rectify the actions described above by providing complete monetary
 13 relief, agreeing to be bound by Sony's legal obligations and to give notice to all affected customers
 14 of their intent to do so. Plaintiffs Johnson has not received a response from Sony and Sony has failed
 15 to take the actions demanded to rectify its violation of the CLRA. Therefore, California Plaintiffs,
 16 individually and on behalf of the other California Subclass members, now seek damages for such
 17 unfair and deceptive practices pursuant to Cal. Civ. Code §1782.

18 **COUNT 4**

19 **Violation of Cal. Civ. Code § 1798.80 *et seq.*** 20 **(On Behalf of California Plaintiffs Arthur Howe and Kyle Johnson** 21 **and the California Subclass)**

22 186. California Plaintiffs Arthur Howe and Kyle Johnson, individually and on behalf of
 23 the other California Subclass members, repeat, reallege, and incorporate by reference the allegations
 24 contained in paragraphs 1-145 above, as though fully stated herein.

25 187. Section 1798.82 of the California Civil Code provides, in pertinent part, as follows:

26 (a) Any person or business that conducts business in California, and that owns or
 27 licenses computerized data that includes personal information, shall disclose any
 28 breach of the security of the system following discovery or notification of the breach
 in the security of the data to any resident of California whose unencrypted personal
 information was, or is reasonably believed to have been, acquired by an unauthorized
 person. The disclosure shall be made in the most expedient time possible and without
 unreasonable delay, consistent with the legitimate needs of law enforcement, as

1 provided in subdivision (c), or any measures necessary to determine the scope of the
2 breach and restore the reasonable integrity of the data system.

3 (b) Any person or business that maintains computerized data that includes personal
4 information that the person or business does not own shall notify the owner or
5 licensee of the information of any breach of the security of the data immediately
6 following discovery, if the personal information was, or is reasonably believed to
7 have been, acquired by an unauthorized person.

8 (c) The notification required by this section may be delayed if a law enforcement
9 agency determines that the notification will impede a criminal investigation. The
10 notification required by this section shall be made after the law enforcement agency
11 determines that it will not compromise the investigation.

12 (d) Any person or business that is required to issue a security breach notification
13 pursuant to this section shall meet all of the following requirements:

14 (1) The security breach notification shall be written in plain language.

15 (2) The security breach notification shall include, at a minimum, the
16 following information:

17 (A) The name and contact information of the reporting person or
18 business subject to this section.

19 (B) A list of the types of personal information that were or are
20 reasonably believed to have been the subject of a breach.

21 (C) If the information is possible to determine at the time the notice is
22 provided, then any of the following: (i) the date of the breach, (ii) the
23 estimated date of the breach, or (iii) the date range within which the
24 breach occurred. The notification shall also include the date of the
25 notice.

26 (D) Whether notification was delayed as a result of a law
27 enforcement investigation, if that information is possible to determine
28 at the time the notice is provided.

(E) A general description of the breach incident, if that information is
possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit
reporting agencies if the breach exposed a social security number or a
driver's license or California identification card number.

* * *

(f) Any person or business that is required to issue a security breach notification
pursuant to this section to more than 500 California residents as a result of a single
breach of the security system shall electronically submit a single sample copy of that
security breach notification, excluding any personally identifiable information, to the
Attorney General. A single sample copy of a security breach notification shall not be
deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

188. The Data Breach constituted a “breach of the security system” of Sony.

189. Sony unreasonably delayed informing anyone about the breach of security of California Subclass members’ confidential and non-public information after Sony knew the Data Breach had occurred.

190. Defendants failed to disclose to California Subclass members, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Personal Information when they knew or reasonably believed such information had been compromised.

191. Upon information and belief, no law enforcement agency instructed Sony that notification to California Subclass members would impede investigation.

192. Pursuant to Section 1798.84 of the California Civil Code:

(a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.

(b) Any customer injured by a violation of this title may institute a civil action to recover damages.

(c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars (\$3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars (\$500) per violation for a violation of Section 1798.83.

* * *

(e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

193. As a result of Sony’s violation of Cal. Civ. Code § 1798.82, California Subclass members incurred economic damages relating to expenses for credit monitoring, loss of use and value of Sony Online Services, loss of use and value of prepaid Third-Party Services, and diminution of the value of their PS3s and/or PSPs.

194. California Plaintiffs, individually and on behalf of the other California Subclass members, seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to: (a) damages suffered by California Subclass members as alleged above; (b) statutory damages for Sony's willful, intentional, and/or reckless violation of Cal. Civ. Code § 1798.83; and (c) equitable relief.

195. California Plaintiffs, individually and on behalf of the other California Subclass members, also seek reasonable attorneys' fees and costs under Cal. Civ. Code §1798.84(g).

COUNT 5

**Negligence under California Law
(On Behalf of California Plaintiffs Arthur Howe and Kyle Johnson
and the California Subclass)**

196. California Plaintiffs Arthur Howe and Kyle Johnson, individually and on behalf of the other California Subclass members, repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1-145 above, as though fully stated herein.

197. Sony owed a duty to Plaintiff Howe, Plaintiff Johnson, and the other California Subclass members to exercise reasonable care in safeguarding and protecting their Personal Information in its possession from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Sony's security systems to ensure that Plaintiff Howe's, Plaintiff Johnson's, and the other California Subclass members' Personal Information in Sony's possession was adequately secured and protected. Sony further had a duty to implement processes that would detect a breach of its security system in a timely manner.

198. Sony had a duty to timely disclose to Plaintiff Howe, Plaintiff Johnson, and the other California Subclass members that their Personal Information had been or was reasonably believed to have been compromised. Timely disclosure was appropriate so that, among other things, Plaintiff Howe, Plaintiff Johnson, and the other California Subclass members could take appropriate measures to avoid unauthorized charges to their credit/debit card accounts, cancel or change usernames and passwords on compromised accounts, and monitor their account information and credit reports for fraudulent activity.

1 199. Sony breached its duty to exercise reasonable care in safeguarding and protecting
2 Plaintiff Howe's, Plaintiff Johnson's, and the other California Subclass members' Personal
3 Information in its possession by failing to adopt, implement, and maintain adequate security
4 measures to safeguard their Personal Information; failing to adequately monitor the security of the
5 Network; allowing unauthorized access to their Personal Information stored on the Network; and
6 failing to recognize in a timely manner that the Network had been breached.

7 200. Sony breached its duty to timely disclose that Plaintiff Howe's, Plaintiff Johnson's,
8 and the other California Subclass members' Personal Information in its possession had been, or was
9 reasonably believed to have been, stolen or compromised.

10 201. Sony's failure to comply with industry regulations, such as PCI DSS, and the delay
11 between the date of intrusion and the date Sony informed customers of the Data Breach further
12 evidence Sony's negligence in failing to exercise reasonable care in safeguarding and protecting
13 Plaintiff Howe's, Plaintiff Johnson's, and the other California Subclass members' Personal
14 Information in its possession.

15 202. But for Sony's wrongful and negligent breach of its duties owed to Plaintiff Howe,
16 Plaintiff Johnson, and the other California Subclass members their Personal Information would not
17 have been compromised, and Sony Online Services would not have been shut down for extended
18 periods of time.

19 203. The injury and harm suffered by Plaintiff Howe, Plaintiff Johnson, and the other
20 California Subclass members was the reasonably foreseeable result of Sony's failure to exercise
21 reasonable care in safeguarding and protecting Plaintiff Howe's, Plaintiff Johnson's, and the other
22 California Subclass members' Personal Information within its possession. Sony knew or should have
23 known that its systems and technologies for processing and securing Plaintiff Howe's, Plaintiff
24 Johnson's, and the other California Subclass members' Personal Information had security
25 vulnerabilities.

26 204. A special relationship exists between the parties that allows for the recovery of
27 economic loss in this case, as articulated herein.

28

1 205. Defendants developed Sony Online Services for users of PS3s and PSPs, such as
2 Plaintiffs Howe and Johnson and the other California Subclass members, and advertised Sony
3 Online Services for registration and use. Sony intended this transaction to affect Plaintiffs Howe and
4 Johnson and the other California Subclass members and required them to provide Personal
5 Information, while indicating that Sony had reasonable security measures to protect this Personal
6 Information, and encouraging users to register for sub-accounts for other individuals, like their
7 children.

8 206. It was foreseeable that Plaintiffs Howe and Johnson and the other California Subclass
9 members would suffer harm if Sony did not provide adequate, reasonable, and industry-standard
10 security, because Sony collected and retained sensitive Personal Information from Plaintiff Howe
11 and Johnson and the other California Subclass members. Moreover, Sony had experienced security
12 issues prior to the Data Breach, was aware that Sony Online Services and the Network had serious
13 security vulnerabilities, and has even admitted such.

14 207. As described herein, Plaintiffs Howe and Johnson and the other California Subclass
15 members suffered injuries as a result of the Data Breach, including expenses for credit monitoring,
16 loss of use and value of Sony Online Services, loss of use and value of prepaid Third-Party Services,
17 and diminution of the value of their PS3s and/or PSPs.

18 208. These injuries were a direct result of Sony's lack of adequate, reasonable and
19 industry-standard security measures. Had Sony implemented adequate, reasonable and industry-
20 standard security measures (such as the security implemented by Sony with regards to its own
21 proprietary network), Plaintiffs Howe and Johnson and the other California Subclass members would
22 not have suffered the injuries alleged, as the Data Breach would likely not have occurred.

23 209. Defendants' conduct warrants moral blame, as Sony collected Plaintiff Howe's,
24 Plaintiff Johnson's, and the other California Subclass members' sensitive Personal Information and
25 promised to take "reasonable measures" to protect such Personal Information, but failed to do so.

26 210. Holding Sony accountable for its negligence here will require it and similar
27 companies that obtain and retain sensitive consumer personal information to price into their security
28

1 practices the cost of implementing and maintaining reasonable, adequate, and industry-standard
2 security measures to protect such personal information.

3 211. As a result of Sony's negligence, Plaintiff Howe, Plaintiff Johnson, and the other
4 California Subclass members incurred economic damages relating to expenses for credit monitoring,
5 loss of use and value of Sony Online Services, loss of use and value of prepaid Third-Party Services,
6 and diminution of the value of their PS3s and/or PSPs.

7 **COUNT 6**

8 **Violations of the Florida Deceptive and Unfair Trade Practices Act,** 9 **Fla. Stat. § 501.201 *et seq.*** 10 **(On Behalf of Florida Plaintiffs Scott Lieberman and Adam Schucher** 11 **and the Florida Subclass)**

12 212. Florida Plaintiffs Lieberman and Schucher, individually and on behalf of the other
13 Florida Subclass members, hereby incorporate by reference the previous allegations in paragraphs 1-
14 145 as if fully set forth herein.

15 213. This cause of action is brought on behalf of the Florida Plaintiffs and the Florida
16 Subclass pursuant to the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§501.201, *et*
17 *seq.* ("FDUTPA"). The stated purpose of FDUTPA is to "protect the consuming public . . . from
18 those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or
19 practices in the conduct of any trade or commerce." Fla. Stat. §501.202(2).

20 214. Florida Plaintiffs Lieberman and Schucher and the other members of the Florida
21 Subclass are consumers as defined by Fla. Stat. §501.203. PS3s, PSPs, and Sony Online Services
22 are goods and/or services within the meaning of FDUTPA. Defendants are engaged in trade or
23 commerce within the meaning of FDUTPA.

24 215. Fla. Stat. §501.204(1) declares unlawful "[u]nfair methods of competition,
25 unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade
26 or commerce."

27 216. Fla. Stat. §501.204(2) states that "due consideration and great weight shall be given to
28 the interpretations of the Federal Trade Commission and the federal courts relating to [section]
5(a)(1) of the Federal Trade Commission Act." Defendants' unfair and deceptive practices are likely

1 to mislead – and have misled – consumers acting reasonably in the circumstances and violate Fla.
2 Stat. §500.04 and 21 U.S.C. §343.

3 217. Defendants have violated FDUTPA by engaging in the unfair and deceptive practices
4 as described herein which offend public policies and are immoral, unethical, unscrupulous and
5 substantially injurious to consumers.

6 218. Florida Plaintiffs Lieberman and Schucher and the other members of the Florida
7 Subclass have been aggrieved by Defendants’ unfair and deceptive practices in that they registered
8 with, and sent their Personal Information to, Sony Online Services after exposure to Defendants’
9 false and misleading representations regarding the security of Sony Online Services.

10 219. The damages suffered by Florida Plaintiffs Lieberman and Schucher and the other
11 members of the Florida Subclass were directly and proximately caused by the deceptive, misleading
12 and unfair practices of Defendants, as more fully described herein.

13 220. Pursuant to Fla. Stat. §501.211(1), Florida Plaintiffs Lieberman and Schucher,
14 individually and on behalf of the Florida Subclass, seek a declaratory judgment and court order
15 enjoining the above-described wrongful acts and practices of Defendants and for restitution and
16 disgorgement.

17 221. Additionally, pursuant to Fla. Stat. §§501.211(2) and 501.2105, Florida Plaintiffs
18 Lieberman and Schucher, individually and on behalf of the Florida Subclass, make claims for
19 damages, attorneys’ fees and costs.

20 **COUNT 7**

21 **Breach of Warranty Under Florida Law** 22 **(On Behalf of Florida Plaintiffs Scott Lieberman and Adam Schucher** **and the Florida Subclass)**

23 222. Florida Plaintiffs Lieberman and Schucher , individually and on behalf of the other
24 Florida Subclass members, hereby incorporate by reference the previous allegations in paragraphs 1-
25 145 as if fully set forth herein.

26 223. The warranties and representations disseminated by Defendants regarding the security
27 of Sony Online Services were, and are, affirmations of fact and/or promises with regard to the
28 performance and quality of the product and/or service. These warranties and representations,

1 formed, in whole or in part, the basis of the bargain between Defendants and the members of the
2 Florida Subclass, and constituted express warranties that Sony Online Services would conform
3 thereto. As described above, Sony Online Services did not conform with these warranties and
4 representations.

5 224. Defendants provided limited warranties to Florida Plaintiffs and the other members of
6 the Florida Subclass, which Defendants breached and failed to honor. To the extent there are any
7 time and content limitations contained in those limited warranties, such limitations are also
8 unconscionable and grossly inadequate to protect Florida Plaintiffs and the other members of the
9 Florida Subclass. Among other things, the members of the Florida Subclass had no meaningful
10 choice in determining those time and content limitations; the terms of the limited warranties
11 unreasonably favored Defendants over the members of the Florida Subclass; a gross disparity in
12 bargaining power existed as between Defendants and the members of the Florida Subclass; and
13 Defendants knew that Sony Online Services' security was inadequate and would fail to provide the
14 promised security.

15 225. By virtue of its knowledge of the inadequacy of the Sony Online Services' security,
16 Defendants have received notice of the breach of the warranties.

17 226. The element of privity, if applicable, exists between Defendants and the members of
18 the Florida Subclass because, *inter alia*: (i) Defendants have had direct written communications
19 with the members of the Florida Subclass with regard to Sony Online Services in the form of
20 standardized warranty forms; (ii) the Florida Plaintiffs registered for Sony Online Services directly
21 with Defendants; (iii) Defendants marketed Sony Online Services to and communicated directly
22 with Florida Plaintiffs and the other members of the Florida Subclass; and (iv) Defendants entered
23 into contracts with members of the Florida Subclass in connection with the assurance of warranties.

24 227. As a result of the foregoing, Florida Plaintiffs and the other members of the Florida
25 Subclass have suffered damages that were directly and proximately caused by the inadequate
26 security of the Network by Defendants.

COUNT 8

**Breach of Implied Warranty Under Florida Law
(On Behalf of Florida Plaintiffs Scott Lieberman and Adam Schucher
and the Florida Subclass)**

228. Florida Plaintiffs Lieberman and Schucher , individually and on behalf of the other Florida Subclass members, hereby incorporate by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

229. Defendants impliedly represented and warranted that Sony Online Services provided adequate security of Personal Information provided by Florida Plaintiffs Lieberman and Schucher and the other members of the Florida Subclass.

230. Defendants breached these representations and implied warranties. Defendants made and/or allowed these misrepresentations to be made with the intent of inducing members of the Florida Subclass to register with, and send their Personal Information to, Sony Online Services. If Florida Plaintiffs and the other members of the Florida Subclass, as reasonable persons, known the true facts regarding the inadequate security of Sony Online Services, they would not have purchased, registered with, or sent their Personal Information to Sony Online Services, or they would not have paid the prices they paid for same.

231. By virtue of its knowledge of the inadequate security of Sony Online Services, Defendants have received notice of the breach of the warranties.

232. The element of privity, if applicable, exists between Defendants and the members of the Florida Subclass because, *inter alia*: (i) Defendants have had direct written communications with the members of the Florida Subclass with regard to Sony Online Services the form of standardized warranty forms; (ii) the members of the Florida Subclass registered for Sony Online Services directly with Defendants; (iii) Defendants marketed Sony Online Services to and communicated directly with Florida Plaintiffs and the other members of the Florida Subclass; and (iv) Defendants entered into contracts with the members of the Florida Subclass in connection with the assurance of warranties.

233. The damages suffered by Florida Plaintiffs and the other Florida Subclass members were directly and proximately caused by the inadequate security of Sony Online Services.

COUNT 9

**Negligent Misrepresentation Under Florida Law
(On Behalf of Florida Plaintiffs Scott Lieberman and Adam Schucher
and the Florida Subclass)**

234. Florida Plaintiffs Lieberman and Schucher, individually and on behalf of the other Florida Subclass members, hereby incorporate by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

235. Defendants negligently and recklessly misrepresented various material facts regarding the quality and character of Sony Online Services, under circumstances where Defendants either knew or reasonably should have known that the representations were not true. These misrepresentations were contained in various advertising, packaging, and correspondence from Defendants, and such misrepresentations were further reiterated and disseminated by the officers, agents, representatives, servants, or employees of Defendants acting within the scope of their authority.

236. In reliance upon these misrepresentations, Florida Plaintiffs and the other members of the Florida Subclass purchased registered with, and sent their Personal Information to Sony Online Services with the expectation that there was adequate security of Personal Information on Sony Online Services.

237. Had Florida Plaintiffs and the other members of the Florida Subclass, as reasonable persons, known of the inadequate security of Sony Online Services, they would not have registered with, or sent their Personal Information to Sony Online Services, or they would not have paid the prices they paid for same.

238. As a direct and proximate consequence of Defendants' negligent misrepresentations, Florida Plaintiffs and the other members of the Florida Subclass have been injured.

COUNT 10

**Unjust Enrichment Under Florida Law
(On Behalf of Florida Plaintiffs Scott Lieberman and Adam Schucher
and the Florida Subclass)**

239. Florida Plaintiffs Lieberman and Schucher , individually and on behalf of the other Florida Subclass members, hereby incorporate by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

240. Florida Plaintiffs Lieberman and Schucher and the other members of the Florida Subclass conferred a benefit on Defendants by purchasing, registering with, and/or sending their Personal Information to Sony Online Services.

241. Defendants have been unjustly enriched in retaining the revenues derived from the Florida Subclass members' registering with, and sending their Personal Information to Sony Online Services and purchases of various games and downloads via Sony Online Services, which retention under these circumstances is unjust and inequitable because Defendants misrepresented that the Network had adequate security. Moreover, by making these misrepresentations, Defendants caused injuries to Florida Plaintiffs and the other members of the Florida Subclass because: (a) they would not have registered with, or sent their Personal Information to, Sony Online Services on the same terms if the true facts regarding the inadequate security of the Network were known; and (b) their PS3s, PSPs, and Sony Online Services did not have the quality, security or value as promised.

242. Because Defendants' retention of the non-gratuitous benefit conferred on it by Florida Plaintiffs and the other members of the Florida Subclass is unjust and inequitable, Defendants must pay restitution to Florida Plaintiffs and the other members of the Florida Subclass for their unjust enrichment, as ordered by the Court.

243. Florida Plaintiffs and the other members of the Florida Subclass have no adequate remedy at law.

COUNT 11

**Negligence Under Florida Law
(On Behalf of Florida Plaintiffs Scott Lieberman and Adam Schucher
and the Florida Subclass)**

244. Florida Plaintiffs Lieberman and Schucher, individually and on behalf of the other Florida Subclass members, hereby incorporate by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

245. By virtue of aforementioned acts, Defendants in requesting, gathering and promising to secure the Personal Information of Florida Plaintiffs Lieberman and Schucher and the other members of the Florida Subclass had a duty to Florida Plaintiffs Lieberman and Schucher and the other members of the Florida Subclass to do so in a reasonable manner consistent with industry standards, to ensure that Sony Online Services were secure, and that Personal Information was secure from theft or misuse.

246. Defendants knew or reasonably should have known that the Network and Personal Information stored thereon was not secure.

247. Defendants breached their duty to of Florida Plaintiffs Lieberman and Schucher and the other members of the Florida Subclass by failing to adequately secure Sony Online Services and placing their Personal Information at risk of theft or misuse.

248. Defendant's negligence is independent of any contractual relationship between the Defendants and Florida Plaintiffs Lieberman and Schucher and the other members of the Florida Subclass.

249. As a direct and proximate result of Defendants' negligence, the failure to adequately secure Sony Online Services and the Personal Information held on the Network has caused economic injury and property damage to Florida Plaintiffs Lieberman and Schucher and the other members of the Florida Subclass.

COUNT 12

**Breach of Implied Warranty Under Massachusetts State Law,
M.G.L. §§ 2-314, 2-315
(On Behalf of Massachusetts Plaintiff Robert Bova and the Massachusetts Subclass)**

250. Massachusetts Plaintiff Robert Bova, individually and on behalf of the other Massachusetts Subclass members, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

251. This cause of action is brought by Massachusetts Plaintiff Robert Bova, individually and on behalf of the other Massachusetts Subclass members, pursuant to Massachusetts State Law §2-314 for breach of implied warranty.

252. By creating, marketing and selling PS3s, PSPs, and Sony Online Services, Defendants, in violation of Mass. Gen. Law §2-314, impliedly represented and warranted that the Network was merchantable, fit for its intended purpose, and provided adequate security of Personal Information provided by Massachusetts Plaintiff Robert Bova and the other Massachusetts Subclass members.

253. Defendants breached these representations and implied warranties. As described more fully above, the Network was not merchantable, fit for its intended purpose, and did not provide adequate security of Personal Information provided by Massachusetts Plaintiff Robert Bova and the other Massachusetts Subclass members. If Massachusetts Plaintiff Robert Bova and the other Massachusetts Subclass members had known the true facts regarding the inadequate security of Sony Online Services, they would not have purchased a PS3, PSP, and/or registered for Sony Online Services.

254. By virtue of their knowledge of the inadequate security of Sony Online Services, Defendants have received notice of the breach of the warranties.

255. The damages suffered by Massachusetts Plaintiff Robert Bova and the other Massachusetts Subclass members were directly and proximately caused by the inadequate security of Sony Online Services and the resulting breach of implied warranties.

COUNT 13

**Unjust Enrichment Under Massachusetts Law
(On Behalf of Massachusetts Plaintiff Robert Bova and the Massachusetts Subclass)**

256. Massachusetts Plaintiff Robert Bova, individually and on behalf of the other Massachusetts Subclass members, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

257. Massachusetts Plaintiff Robert Bova and the other Massachusetts Subclass members conferred benefits on Sony by purchasing PS3s, PSPs, and/or Sony Online Services, and registering for Sony Online Services.

258. Massachusetts Plaintiff Robert Bova and the other Massachusetts Subclass members, however, were deprived of the full value of their PS3s, PSPs, and Sony Online Services due to Sony's disabling of Sony Online Services.

259. Defendants have been unjustly enriched by the revenues from Massachusetts Plaintiff Robert Bova's and the other Massachusetts Subclass members' purchases of the PS3, PSP, and/or Sony Online Services, registrations on Sony Online Services, and purchases of various games and downloads via Sony Online Services. This enrichment is unjust and inequitable because Defendants misrepresented that Sony Online Services had adequate security. Moreover, by making these misrepresentations, Defendants caused injuries to Massachusetts Plaintiff Robert Bova and the other members of the Massachusetts Subclass because: (a) they would not have purchased the PS3, PSP, and/or Sony Online Services and/or registered with Sony Online Services on the same terms if the true facts regarding the inadequate security of Sony Online Services were known; and (b) their PS3s, PSPs, and Sony Online Services did not have the quality, security or value as promised.

260. Defendants' retention of the non-gratuitous benefit conferred on it by Massachusetts Plaintiff Robert Bova and the other members of the Massachusetts Subclass is unjust and inequitable, and therefore Defendants must pay restitution to Massachusetts Plaintiff and the other Massachusetts Subclass members as ordered by the Court.

261. Massachusetts Plaintiff Robert Bova and the other Massachusetts Subclass members have no adequate remedy at law.

COUNT 14**Negligence Under Massachusetts Law
(On Behalf of Massachusetts Plaintiff Robert Bova and the Massachusetts Subclass)**

262. Massachusetts Plaintiff Robert Bova, individually and on behalf of the other Massachusetts Subclass members, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

263. Sony owed a duty to Massachusetts Plaintiff Robert Bova and the other Massachusetts Subclass members to exercise reasonable care in safeguarding and protecting their Personal Information in its possession from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Sony's security systems to ensure that Massachusetts Plaintiff Robert Bova's and the other Massachusetts Subclass members' Personal Information in Sony's possession was adequately secured and protected. Sony further had a duty to implement processes that would detect a breach of its Network in a timely manner.

264. Sony had a duty to timely disclose to Massachusetts Plaintiff Robert Bova and the other Massachusetts Subclass members that their Personal Information had been or was reasonably believed to have been compromised. Timely disclosure was appropriate so that, among other things, Massachusetts Plaintiff Bova and the other members of the Massachusetts Subclass Class could take appropriate measures to avoid unauthorized charges to their credit/debit card accounts, cancel or change usernames and passwords on compromised accounts, and monitor their account information and credit reports for fraudulent activity.

265. Sony breached its duty to exercise reasonable care in safeguarding and protecting Massachusetts Plaintiff Robert Bova's and the other Massachusetts Subclass members' Personal Information in its possession by failing to adopt, implement, and maintain adequate security measures to safeguard Massachusetts Plaintiff Robert Bova's and the other Massachusetts Subclass members' Personal Information; failing to adequately monitor the security of Sony Online Services; allowing unauthorized access to Massachusetts Plaintiff Robert Bova's and the other Massachusetts

1 Subclass members' Personal Information stored on the Network; and failing to recognize in a timely
2 manner that the Network had been breached.

3 266. Sony breached its duty to timely disclose that Massachusetts Plaintiff Robert Bova
4 and the other Massachusetts Subclass members' Personal Information in its possession had been, or
5 was reasonably believed to have been, stolen or compromised.

6 267. Sony's failure to comply with industry regulations, such as PCI DSS, and the delay
7 between the date of intrusion and the date Sony informed customers of the Data Breach further
8 evidence Sony's negligence in failing to exercise reasonable care in safeguarding and protecting
9 Massachusetts Plaintiff Robert Bova and the other Massachusetts Subclass members' Personal
10 Information in its possession.

11 268. But for Sony's wrongful and negligent breach of its duties owed to Massachusetts
12 Plaintiff Robert Bova and the other Massachusetts Subclass members, their Personal Information
13 would not have been compromised, and Sony Online Services would not have been shut down for
14 extended periods of time.

15 269. The injury and harm suffered by Massachusetts Plaintiff Robert Bova and the other
16 Massachusetts Subclass members was the reasonably foreseeable result of Sony's failure to exercise
17 reasonable care in safeguarding and protecting Massachusetts Plaintiff Robert Bova's and the other
18 Massachusetts Subclass members' Personal Information within its possession. Sony knew or should
19 have known that its systems and technologies for processing and securing Massachusetts Plaintiff
20 Robert Bova's and the other Massachusetts Subclass members' Personal Information had security
21 vulnerabilities.

22 270. As a result of Sony's negligence, Massachusetts Plaintiff Robert Bova and the other
23 Massachusetts Subclass members incurred economic damages relating to expenses for credit
24 monitoring, loss of use and value of Sony Online Services, loss of use and value of prepaid Third-
25 Party Services, and diminution of the value of their PS3s and/or PSPs.

COUNT 15**Negligent Misrepresentation Under Massachusetts Law
(On Behalf of Massachusetts Plaintiff Robert Bova and the Massachusetts Subclass)**

271. Massachusetts Plaintiff Robert Bova, individually and on behalf of the other Massachusetts Subclass members, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

272. Defendants negligently and recklessly misrepresented various material facts regarding the quality and character of Sony Online Services and the Network, under circumstances where Defendants either knew or reasonably should have known that the representations were not true. These misrepresentations were contained in various advertising, packaging, and correspondence from Defendants.

273. In reliance upon these misrepresentations about the security of the Network, Massachusetts Plaintiff Robert Bova and the other Massachusetts Subclass members purchased PS3s, PSPs, Sony Online Services and/or registered for Sony Online Services.

274. Had Massachusetts Plaintiff Robert Bova and the other Massachusetts Subclass members, as reasonable persons, known of the inadequate security of the Network, they would not have purchased PS3s, PSPs, Sony Online Services and/or registered for Sony Online Services, or they would not have paid the prices they paid for same.

275. As a direct and proximate consequence of Defendants' negligent misrepresentations, Massachusetts Plaintiff Robert Bova and the other Massachusetts Subclass members have suffered the injuries as alleged above.

COUNT 16**Violations of the Michigan Consumer Protection Act,
M.C.L. § 445.901 et seq.
(On Behalf of Michigan Plaintiff Rebecca Mitchell and the Michigan Subclass)**

276. Michigan Plaintiff Rebecca Mitchell, individually and on behalf of the other members of the Michigan Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

1 277. This cause of action is brought by Michigan Plaintiff Mitchell, individually and on
2 behalf of the other Michigan Subclass members, pursuant to the Michigan Consumer Protection Act,
3 M.C.L. § 445.901 *et seq.*

4 278. Plaintiff Mitchell is a person within the meaning of M.C.L. § 445.902(1)(d).

5 279. By providing on-line gaming, video and music services to Michigan consumers for
6 personal, family and/or household purposes, Defendants are engaged in trade or commerce within
7 the meaning of M.C.L. § 445.902(g).

8 280. M.C.L. § 445.903 declares unlawful “unfair, unconscionable, or deceptive acts or
9 practices in the conduct of trade or commerce.”

10 281. As described herein, Defendants have engaged unfair, unconscionable and/or
11 deceptive acts by misleading the consuming public into believing that their Personal Information
12 would be safe upon transmission to Defendants when in fact Defendants knew that their security
13 systems were woefully inadequate. Such conduct violates M.C.L. §§ 445.903(1)(c),(e),(bb),and (cc)

14 282. Michigan Plaintiff Mitchell and the other members of the Michigan Subclass are
15 persons who have suffered loss under M.C.L. § 445.911(3) in that they have suffered the loss of
16 privacy and/or Personal Information and, further, have paid for PS3s, PSPs, Sony Online Services
17 and/or registered with Sony Online Services after being exposed to Defendants’ materially
18 misleading representations regarding the security of Sony Online Services.

19 283. The damages suffered by Michigan Plaintiff Mitchell and the other members of the
20 Michigan Subclass were directly and proximately caused by the materially misleading acts and/or
21 practices of Defendants, as more fully described herein.

22 284. Pursuant to M.C.L. § 445.911(1)(a), Michigan Plaintiff Mitchell, individually and on
23 behalf of the other members of the Michigan Subclass, seeks a declaratory judgment that
24 Defendants’ conduct as described herein violates M.C.L. §§ 445.903(1)(c),(e),(bb),and (cc).

25 285. On information and belief, Defendants continue to misrepresent the adequacy of their
26 security systems and will continue to do so unless retained by Court order. Accordingly, pursuant to
27 M.C.L. § 445.911(1)(b), Michigan Plaintiff Mitchell, individually and on behalf of the other
28 members of the Michigan Subclass, seeks an order forbidding Defendants from representing that

1 they have security systems that adequately protect the Personal Information of consumers, including
2 Michigan consumers.

3 286. Pursuant to M.C.L. § 445.911(3), Michigan Plaintiff Mitchell, individually and on
4 behalf of the other members of the Michigan Subclass, seeks an order: (a) requiring Defendants to
5 reimburse Plaintiff Mitchell and the other members of the Michigan Subclass their actual damages;
6 (b) requiring Defendants to provide adequate security systems for purposes of protecting Michigan
7 consumers' Personal Information in the possession and control of Defendants; (c) striking or limiting
8 the application of unconscionable clauses of contract that Defendants invoke to limit their liability
9 for violations of the Michigan Consumer Protection Act; and (d) awarding all other appropriate
10 relief, including but not limited to attorneys' fees and costs as part of any common fund awarded to
11 the Michigan Subclass.

12 287. In the alternative, in the event the Court declines to certify a Michigan Subclass,
13 Plaintiff Mitchell, as an individual plaintiff, seeks an award of her actual damages or \$250.00,
14 whichever is greater, together with reasonable attorneys' fees as provided for under M.C.L. §
15 445.911(2).

16 **COUNT 17**

17 **Breach of Warranty Under Michigan Law** 18 **(On Behalf of New York Plaintiff Rebecca Mitchell and the Michigan Subclass)**

19 288. Michigan Plaintiff Rebecca Mitchell, individually and on behalf of the other members
20 of the Michigan Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-
21 145 as if fully set forth herein.

22 289. The warranties and representations disseminated by Defendants regarding the security
23 of Sony Online Services were, and are, affirmations of fact and/or promises with regard to the
24 performance and quality of the product and/or service. These warranties and representations, formed,
25 in whole or in part, the basis of the bargain between Defendants and members of the Michigan
26 Subclass, and constituted express warranties that Sony Online Services would conform thereto. As
27 described above, Sony Online Services did not conform to these warranties and representations.
28

1 290. Defendants provided limited warranties to Michigan Plaintiff Mitchell and the other
2 members of the Michigan Subclass, which Defendants breached and failed to honor. To the extent
3 that there are any time and content limitations contained in those limited warranties, such limitations
4 are unconscionable and grossly inadequate to protect the Michigan Plaintiff and the other members
5 of the Michigan Subclass. Among other things, members of the Michigan Subclass had no
6 meaningful choice in determining those time and content limitations; the terms of the limited
7 warranties unreasonably favored Defendants over members of the Michigan Subclass; a gross
8 disparity in bargaining power existed as between Defendants and members of the Michigan
9 Subclass; and Defendants knew Sony Online Services' security was inadequate and would fail to
10 provide the promised security.

11 291. By virtue of its knowledge of the inadequacy of Sony Online Services' security,
12 Defendants have received notice of the breach of the warranties.

13 292. The element of privity, if applicable, exists between Defendants and the members of
14 the Michigan Subclass because, *inter alia*: (i) Defendants have had direct written communications
15 with members of the Michigan Subclass with regard to Sony Online Services in the form of
16 standardized warranty forms; (ii) Michigan Plaintiff Mitchell and the other members of the Michigan
17 Subclass registered for Sony Online Services directly with Defendants; (iii) Defendants marketed
18 Sony Online Services to and communicated directly with Michigan Plaintiff Mitchell and the other
19 members of the Michigan Subclass; and (iv) Defendants entered into contracts with members of the
20 Michigan Subclass in connection with the assurance of warranties.

21 293. As a result of the foregoing, Michigan Plaintiff Mitchell and the other members of the
22 Michigan Subclass have suffered damages that were directly and proximately caused by the
23 inadequate security of Sony Online Services by Defendants.

COUNT 18

**Breach of Implied Warranty Under Michigan Law
(On Behalf of Michigan Plaintiff Rebecca Mitchell and the Michigan Subclass)**

294. Michigan Plaintiff Rebecca Mitchell, individually and on behalf of the other members of the Michigan Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

295. Defendants impliedly represented and warranted that Sony Online Services provided adequate security of Personal Information provided by Michigan Plaintiff Mitchell and the other members of the Michigan Subclass.

296. Defendants breached these representations and implied warranties. Defendants made and/or allowed these misrepresentations to be made with the intent of inducing members of the Michigan Subclass to purchase PS3s, PSPs, Sony Online Services and/or to register for Sony Online Services. If Michigan Plaintiff Mitchell and the other members of the Michigan Subclass, as reasonable persons, known the true facts regarding the inadequate security of Sony Online Services, they would not have purchased PS3s, PSPs, Sony Online Services and/or registered for Sony Online Services, or they would not have paid the prices they paid for same.

297. By virtue of its knowledge of the inadequate security of Sony Online Services, Defendants have received notice of the breach of the warranties.

298. The element of privity, if applicable, exists between Defendants and members of the Michigan Subclass because, *inter alia*: (i) Defendants have had direct written communications with members of the Michigan Subclass with regard to Sony Online Services in the form of standardized warranty forms; (ii) members of the Michigan Subclass registered for Sony Online Services directly with Defendants; (iii) Defendants marketed Sony Online Services to and communicated directly with Michigan Plaintiff Mitchell and the other members of the Michigan Subclass; and (iv) Defendants entered into contracts with members of the Michigan Subclass in connection with the assurance of warranties.

299. The damages suffered by the Michigan Plaintiff Mitchell and the other members of the Michigan Subclass were directly and proximately caused by the inadequate security of Sony Online Services.

COUNT 19

**Negligent Misrepresentation Under Michigan Law
(On Behalf of Michigan Plaintiff Rebecca Mitchell and the Michigan Subclass)**

300. Michigan Plaintiff Rebecca Mitchell, individually and on behalf of the other members of the Michigan Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

301. In the course of their dealings with Michigan Plaintiff Mitchell and the other members of the Michigan Subclass, Defendants had a duty to supply accurate and non-misleading information concerning the security of Sony Online Services. Further, Defendants had a duty to exercise reasonable care and competence in communicating the information about the security of the Sony Online Services to Michigan Plaintiff Mitchell and the other members of the Michigan Subclass.

302. Defendants breached their duty and supplied false information to be used by Michigan Plaintiff Mitchell and the other members of the Michigan Subclass for their guidance in their dealings with Defendants, namely that Defendants had adequate security systems that would protect the Personal Information of Michigan Plaintiff Mitchell and the other members of the Michigan Subclass when in fact Defendants knew or should have known that they did not have adequate security systems at the time such representations were made.

303. This false information was justifiably relied upon by Michigan Plaintiff Mitchell and the other members of the Michigan Subclass and induced them to register with, and send their Personal Information to Defendants, thereby proximately causing the Michigan Plaintiffs damages -- all of which inured to the benefit of Defendants.

304. As a direct and proximate result of this reliance upon the false information, Michigan Plaintiff Mitchell and the other members of the Michigan Subclass were damaged in an amount which will be proven at trial.

COUNT 20**Innocent Misrepresentation Under Michigan Law
(On Behalf of Michigan Plaintiff Rebecca Mitchell and the Michigan Subclass)**

305. Michigan Plaintiff Rebecca Mitchell, individually and on behalf of the other members of the Michigan Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

306. In the course of their dealings with Michigan Plaintiff Mitchell and the other members of the Michigan Subclass, Defendants supplied false information regarding a material fact, namely that Defendants had adequate security systems that would protect the Personal Information of Michigan Plaintiff Mitchell and the other members of the Michigan Subclass when, in fact, Defendants did have such systems in place at the time such representations were made.

307. Michigan Plaintiff Mitchell and the other members of the Michigan Subclass relied upon Defendants' false information regarding the adequacy of Defendants' security systems. Had Defendants stated the truth regarding Defendants' woefully inadequate security systems, Michigan Plaintiff Mitchell and the other members of the Michigan Subclass would not have purchased their PS3s, PSPs, Sony Online Services and/or registered for Sony Online Services or provided their Personal Information to Defendants.

308. This false information was justifiably relied upon by Michigan Plaintiff Mitchell and the other members of the Michigan Subclass and induced them to purchase PS3s, PSPs, Sony Online Services and/or register on Sony Online Services and to send their Personal Information to Defendants, thereby proximately causing Michigan Plaintiff Mitchell and the other members of the Michigan Subclass damages -- all of which inured to the benefit of Defendants.

309. As a direct and proximate result of this reliance upon the false information, Michigan Plaintiff Mitchell and the other members of the Michigan Subclass were damaged in an amount which will be proven at trial.

COUNT 21**Unjust Enrichment Under Michigan Law
(On Behalf of Michigan Plaintiff Rebecca Mitchell and the Michigan Subclass)**

310. Michigan Plaintiff Rebecca Mitchell, individually and on behalf of the other members of the Michigan Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

311. Michigan Plaintiff Mitchell and the other members of the Michigan Subclass had a direct relationship with Defendants and, in the course of that relationship, conferred a benefit on Defendants by purchasing PS3s, PSPs, Sony Online Services and/or registering on Sony Online Services and by providing their Personal Information to Defendants in doing so.

312. Defendants have been enriched in receiving and retaining the revenues derived from the Michigan Subclass members' purchases of PS3s, PSPs, Sony Online Services and/or registration on Sony Online Services, and purchases of various games and downloads via Sony Online Services. In addition, Defendants have been enriched by receiving and retaining Michigan Plaintiff Mitchell's and the other Michigan Subclass members' Personal Information, which receipt and retention under these circumstances is against equity and good conscience because Defendants misrepresented that Sony Online Services had adequate security.

313. Moreover, by making these misrepresentations and retaining the aforementioned benefits, Defendants caused injuries to Michigan Plaintiff Mitchell and the other members of the Michigan Subclass because: (a) they would not have purchased PS3s, PSPs, Sony Online Services and/or registered with Sony Online Services and provided their Personal Information to Defendants on the same terms if the true facts regarding the inadequate security of Sony Online Services were known; and (b) their PS3s, PSPs, and Sony Online Services did not have the quality, security or value as promised.

COUNT 22

**Violations of the Missouri Merchandising Practices Act,
Mo. Rev. Stat. § 407.010 *et seq.*
(On Behalf of Missouri Plaintiff Christopher Munsterman and the Missouri Subclass)**

314. Missouri Plaintiff Munsterman, individually and on behalf of the other members of the Missouri Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

315. This cause of action is brought on behalf of Missouri Plaintiff Munsterman and the Missouri Subclass pursuant to the Missouri Merchandising Practices Act, Mo. Rev. Stat. §§407.010, *et seq.* (the “Missouri Act”).

316. At all relevant times, Missouri Plaintiff Munsterman, the other members of the Missouri Subclass, and Defendants were “persons” within the meaning of Mo. Rev. Stat. §407.025(1).

317. At all relevant times, Defendants engaged in the “sale or advertisement of any merchandise in trade or commerce” within the meaning of Mo. Rev. Stat. §407.020(1).

318. The Missouri Act prohibits “deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce.” Mo. Rev. Stat. §407.020(1).

319. PS3s, PSPs, and Sony Online Services are “merchandise in trade or commerce” within the meaning of Mo. Rev. Stat. §407.020.1.

320. Because of, among other things, their superior access to information regarding the inadequate security of the Network, Defendants had a legal duty to inform consumers of their products, including Missouri Plaintiff Munsterman and the other members of the Missouri Subclass, of the inadequacy of Sony Online Services’ security.

321. Defendants have, therefore, through their employees, agents, and representatives, engaged in acts, methods or practices of deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression or omission of material facts in connection with advertising and marketing PS3s, PSPs, and Sony Online Services and thereby

1 violated the Missouri Act, all by, among other things, failing to disclose that the security of Personal
2 Information on Sony Online Services was inadequate.

3 322. As a direct and proximate result of Defendants' deception, fraud, false pretense, false
4 promise, misrepresentation, unfair practice or the concealment, suppression or omission of material
5 facts, Missouri Plaintiff Munsterman and the other members of the Missouri Subclass were induced
6 to purchase PS3s, PSPs, Sony Online Services and/or to register with Sony Online Services and had
7 their Personal Information compromised.

8 323. As a direct and proximate result of Defendants' conduct described herein, Missouri
9 Plaintiff Munsterman and the other members of the Missouri Subclass provided their Personal
10 Information to Defendants to be stored on the Network that was handled in such a manner by
11 Defendants as to put their Personal Information at risk for theft and misuse and have otherwise been
12 damaged.

13 324. The conduct of Defendants as set forth herein constitutes unfair or deceptive acts or
14 practices, including Defendants' practices of leading Missouri Plaintiff Munsterman and the other
15 members of the Missouri Subclass to believe that their Personal Information stored on the Network
16 was secure.

17 325. Defendants' conduct as set forth herein was unfair because the acts or practices
18 violate the Missouri Act, Mo. Rev. Stat. chap. 407, established public policy, and because the harm
19 they causes to consumers in Missouri greatly outweighed any benefits associated with those
20 practices.

21 326. Defendants' conduct as set forth herein resulted in loss of money or property to
22 Missouri Plaintiff Munsterman and the other members of the Missouri Subclass.

23 327. Missouri Plaintiff Munsterman, individually and on behalf of the other Missouri
24 Subclass members, seeks actual damages; a declaration that Defendants' conduct violates the
25 Missouri Act, Mo. Rev. Stat. §§407.010, *et seq.*; and injunction prohibiting Defendants from
26 continuing to engage in such unlawful conduct; restitution; pre- and post-judgment interest; and
27 attorneys' fees and costs.

28

333. Missouri Plaintiff Munsterman and the other members of the Missouri Subclass have no adequate remedy at law.

COUNT 24

Breach of Warrant Under Missouri Law
(On Behalf of Missouri Plaintiff Christopher Munsterman and the Missouri Subclass)

334. Missouri Plaintiff Munsterman, individually and on behalf of the other members of the Missouri Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

335. The warranties and representations disseminated by Defendants regarding the security of Sony Online Services were, and are, affirmations of fact and/or promises with regard to the performance and quality of the product and/or service. These warranties and representations, formed, in whole or in part, the basis of the bargain between Defendants and members of the Missouri Subclass, and constituted express warranties that Sony Online Services would conform thereto. As described above, the Missouri Subclass's Sony Online Services did not conform to these warranties and representations.

336. Defendants provided limited warranties to Missouri Plaintiff Munsterman and the other members of the Missouri Subclass, which Defendants breached and failed to honor. To the extent there are any time and content limitations contained in those limited warranties, such limitations are also unconscionable and grossly inadequate to protect Missouri Plaintiff Munsterman and the other members of the Missouri Subclass. Among other things, members of the Missouri Subclass had no meaningful choice in determining those time and content limitations; the terms of the limited warranties unreasonably favored Defendants over members of the Missouri Subclass; a gross disparity in bargaining power existed as between Defendants and members of the Missouri Subclass; and Defendants knew Sony Online Services' security was inadequate and would fail to provide the promised security.

337. By virtue of its knowledge of the inadequacy of Sony Online Services' security, Defendants have received notice of the breach of the warranties.

338. The element of privity, if applicable, exists between Defendants and members of the Missouri Subclass because, *inter alia*: (i) Defendants have had direct written communications with Missouri Plaintiff Munsterman and the other members of the Missouri Subclass with regard to Sony Online Services in the form of standardized warranty forms; (ii) Missouri Plaintiff Munsterman and the other members of the Missouri Subclass registered for Sony Online Services directly with Defendants; (iii) Defendants marketed Sony Online Services to and communicated directly with Missouri Plaintiff Munsterman and the other members of the Missouri Subclass; and (iv) Defendants entered into contracts with members of the Missouri Subclass in connection with the assurance of warranties.

339. As a result of the foregoing, Missouri Plaintiff Munsterman and the other members of the Missouri Subclass have suffered damages that were directly and proximately caused by the inadequate security of Sony Online Services by Defendants.

COUNT 25

**Breach of Implied Warranty Under Missouri Law
(On Behalf of Missouri Plaintiff Christopher Munsterman and the Missouri Subclass)**

340. Missouri Plaintiff Munsterman, individually and on behalf of the other members of the Missouri Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

341. Defendants impliedly represented and warranted that Sony Online Services provided adequate security of Personal Information provided by Missouri Plaintiff Munsterman and the other members of the Missouri Subclass.

342. Defendants breached these representations and implied warranties. Defendants made and/or allowed these misrepresentations to be made with the intent of inducing members of the Missouri Subclass to purchase PS3s, PSPs, Sony Online Services and/or register for Sony Online Services. If Missouri Plaintiff Munsterman and the other members of the Missouri Subclass, as reasonable persons, known the true facts regarding the inadequate security of Sony Online Services, they would not have purchased PS3s, PSPs, Sony Online Services and/or registered for Sony Online Services, or they would not have paid the prices they paid for same.

343. By virtue of its knowledge of the inadequate security of Sony Online Services, Defendants have received notice of the breach of the warranties.

344. The element of privity, if applicable, exists between Defendants and the members of the Missouri Subclass because, *inter alia*: (i) Defendants have had direct written communications with Missouri Plaintiff Munsterman and the other members of the Missouri Subclass with regard to Sony Online Services in the form of standardized warranty forms; (ii) Missouri Plaintiff Munsterman and the other members of the Missouri Subclass registered for Sony Online Services directly with Defendants; (iii) Defendants marketed Sony Online Services to and communicated directly with Missouri Plaintiff Munsterman and the other members of the Missouri Subclass; and (iv) Defendants entered into contracts with Missouri Plaintiff Munsterman and the other members of the Missouri Subclass in connection with the assurance of warranties.

345. The damages suffered by Missouri Plaintiff Munsterman and the other members of the Missouri Subclass were directly and proximately caused by the inadequate security of Sony Online Services.

COUNT 26

Negligent Omission Under Missouri Law
(On Behalf of Missouri Plaintiff Christopher Munsterman and the Missouri Subclass)

346. Missouri Plaintiff Munsterman, individually and on behalf of the other members of the Missouri Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

347. Defendants negligently and recklessly misrepresented various material facts regarding the quality and character of Sony Online Services, under circumstances where Defendants either knew or reasonably should have known that the representations were not true. These material misrepresentations were contained in various advertising, packaging, and correspondence from Defendants, and such misrepresentations were further reiterated and disseminated by the officers, agents, representatives, servants, or employees of Defendants acting within the scope of their authority.

348. Defendants had a legal duty to advise its potential and actual consumers of the inadequate security of Personal Information on Sony Online Services.

349. Notwithstanding said duty, Defendants failed to advise its potential or actual consumers of the inadequate security of Sony Online Services, as described more fully herein.

350. As a direct and proximate result of Defendants' negligence, Missouri Plaintiff Munsterman and the other members of the Missouri Subclass were provided with information regarding the security of Personal Information on Sony Online Services that was false, omitted material information, and/or was highly misleading.

351. Missouri Plaintiff Munsterman and the other members of the Missouri Subclass were ignorant of the true facts regarding the security of Sony Online Services through no fault of their own, and were entitled to rely upon Defendants' characterization of Sony Online Services' data security.

352. The negligent omissions were material in that they induced Missouri Plaintiff Munsterman and the other members of the Missouri Subclass to purchase PS3s, PSPs, and Sony Online Services and/or to register for Sony Online Services.

353. Had Missouri Plaintiff Munsterman and the other members of the Missouri Subclass, as reasonable persons, known of the inadequate security of Sony Online Services, they would not have purchased PS3s, PSPs, Sony Online Services and/or registered for Sony Online Services, or they would not have paid the prices they paid for same.

354. As a direct and proximate result of Defendants' negligent omissions of material fact, Missouri Plaintiff Munsterman and the other members of the Missouri Subclass have been injured.

COUNT 27

Negligence Under Missouri Law

(On Behalf of Missouri Plaintiff Christopher Munsterman and the Missouri Subclass)

355. Missouri Plaintiff Munsterman, individually and on behalf of the other members of the Missouri Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

356. By virtue of aforementioned acts of Defendants, Defendants in requesting, gathering and promising to secure the Personal Information of Missouri Plaintiff Munsterman and the other Missouri Subclass members had a duty to Missouri Plaintiff Munsterman and the other Missouri Subclass members to do so in a reasonable manner consistent with industry standards, to ensure that Sony Online Services were secure, and that Personal Information was secure from theft or misuse.

357. Defendants knew or reasonably should have known that Personal Information held on Sony Online Services was not secure.

358. Defendants breached their duty to of Missouri Plaintiff Munsterman and the Missouri Subclass by failing to adequately secure Sony Online Services and placing their Personal Information at risk of theft or misuse.

359. Defendant's negligence is independent of any contractual relationship between the Defendants and Missouri Plaintiff Munsterman and the other members of the Missouri Subclass.

360. As a direct and proximate result of Defendants' negligence, the failure to adequately secure Sony Online Services and the Personal Information held on the Network has caused economic injury and property damage to Missouri Plaintiff Munsterman and the other members of the Missouri Subclass.

COUNT 28

**Violations of the New Hampshire Consumer Protection Act,
N.H. Rev. Stat. Ann. § 358-A
(On Behalf of New Hampshire Plaintiff Christian Kalled and the New Hampshire Subclass)**

361. New Hampshire Plaintiff Christian Kalled, individually and on behalf of the other members of the New Hampshire Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as though fully set forth herein.

362. This cause of action is brought by New Hampshire Plaintiff Christian Kalled, individually and on behalf of the other New Hampshire Subclass members, under the New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A (hereafter, “NHCPA”).

363. Defendants in this matter are “persons” as defined by N.H. Rev. Stat. Ann. § 358-A:1 and, at all times relevant hereto, were engaged in trade or commerce within the meaning of NHCPA.

1 Additionally, the PS3, PSP, and Sony Online Services are goods and/or services within the meaning
2 of NHCPA.

3 364. The NHCPA prohibits using “any unfair method of competition or any unfair or
4 deceptive act or practice in the conduct of any trade or commerce” within the state. N.H. Rev. Stat.
5 Ann. § 358-A:2. Among the specifically prohibited acts are “[r]epresenting that goods or services
6 have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not
7 have or that a person has a sponsorship, approval, status, affiliation, or connection that such person
8 does not have”; “[r]epresenting that goods or services are of a particular standard, quality, or grade,
9 or that goods are of a particular style or model, if they are of another”; and “[a]dvertising goods or
10 services with intent not to sell them as advertised.” *Id.*

11 365. N.H. Rev. Stat. Ann. § 358-A:11 states that in interpreting the NHCPA, deference
12 should be given to the judicial interpretations and interpretations by the Federal Trade Commission
13 of Section 5(a)(1) the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1).

14 366. Defendants have violated the NHCPA by engaging in the unfair and deceptive
15 practices as described herein which offend public policies and are immoral, unethical, unscrupulous
16 and substantially injurious to consumers. Defendants represented the PS3, PSP, and Sony Online
17 Services had security characteristics, uses, and benefits that they do not have and represented the
18 security of the PS3, PSP, and Sony Online Services was of a particular standard, quality, or grade
19 when it was not.

20 367. New Hampshire Plaintiff Christian Kalled and the other members of the New
21 Hampshire Subclass have been damaged by Defendants’ violations of the NHCPA in that they
22 purchased PS3s, PSPs, Sony Online Services and/or registered with Sony Online Services after
23 exposure to Defendants false and misleading representations regarding the security of PS3s, PSPs,
24 and Sony Online Services.

25 368. The damages suffered by New Hampshire Plaintiff Christian Kalled and the other
26 members of the New Hampshire Subclass were directly and proximately caused by the deceptive,
27 misleading and unfair practices of Defendants, as more fully described herein.

28

369. Pursuant to N.H. Rev. Stat. Ann. § 358-A:10, New Hampshire Plaintiff Christian Kalled, individually and on behalf of the other members of the New Hampshire Subclass, seeks a declaratory judgment and court order enjoining the above-described wrongful acts and practices of Defendants and for restitution and disgorgement.

370. Additionally, pursuant to N.H. Rev. Stat. Ann. § 358-A:10, New Hampshire Plaintiff Christian Kalled, individually and on behalf of the other New Hampshire Subclass members, makes claims for statutory and actual damages, and attorneys' fees and costs. Because the conduct of Defendants as alleged herein was willful or a knowing violation of the NHCPA, New Hampshire Plaintiff Christian Kallad, individually and on behalf of the other members of the New Hampshire Subclass, additionally requests a multiplier of damages as required by N.H. Rev. Stat. Ann. § 358-A:10.

COUNT 29

Breach of Express Warranty Under New Hampshire Law
(On Behalf of New Hampshire Plaintiff Christian Kalled and the New Hampshire Subclass)

371. New Hampshire Plaintiff Christian Kalled, individually and on behalf of the other members of the New Hampshire Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as though fully set forth herein.

372. At all times relevant hereto, by advertising and selling PS3s, PSPs, and Sony Online Services, Defendants made promises about the performance and quality of the security on PS3s, PSPs, and Sony Online Services. New Hampshire Plaintiff Christian Kalled and the other members of the New Hampshire Subclass relied on these express warranties and representations in deciding to purchase PS3s, PSPs, Sony Online Services and/or to register with Sony Online Services, and these express warranties and representations formed, in whole or in part, the basis of the bargain between Defendants and New Hampshire Plaintiff Christian Kalled and the other members of the New Hampshire Subclass. As described above, the PS3, PSP, and Sony Online Services did not conform to these warranties and representations.

373. Defendants provided limited warranties to New Hampshire Plaintiff Christian Kalled and the other members of the New Hampshire Subclass, which Defendants breached and failed to

honor. In the event that those limited warranties contain time and content restrictions, those limitations are unconscionable and grossly inadequate to protect New Hampshire Plaintiff and the other members of the New Hampshire Subclass. Among other things, New Hampshire Plaintiff Christian Kalled and the other New Hampshire Subclass members had no meaningful choice in determining those time and content limitations; the terms of the limited warranties unreasonably favor Defendants over members of the New Hampshire Subclass; there is a gross disparity in bargaining power between Defendants and the members of the New Hampshire Subclass; and Defendants knew Sony Online Services' security was inadequate.

374. If New Hampshire Plaintiff and the other members of the New Hampshire Subclass, as reasonable persons, known the true facts regarding the inadequate security of Sony Online Services, they would not have purchased PS3s, PSPs, Sony Online Services and/or registered with Sony Online Services, or they would not have paid the prices they paid for same.

375. Because Defendants knew of the inadequacy of Sony Online Services' security, Defendants have received notice of the breach of the warranties.

376. As a result of the foregoing, New Hampshire Plaintiff Christian Kalled and the other members of the New Hampshire Subclass have suffered damages that were directly and proximately caused by the breach of express warranties made by Defendants about the security of Sony Online Services.

COUNT 30

**Breach of Implied Warranties Under New Hampshire Law,
N.H. Rev. Stat. Ann. §§ 382-A:3-31, 3-315
(On Behalf of New Hampshire Plaintiff Christian Kalled and the New Hampshire Subclass)**

377. New Hampshire Plaintiff Christian Kalled, individually and on behalf of the other members of the New Hampshire Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as though fully set forth herein.

378. By creating, marketing, and selling PS3s, PSPs, and Sony Online Services, Defendants impliedly represented and warranted that Sony Online Services was merchantable, fit for its intended purpose, and provided adequate security of Personal Information provided by New Hampshire Plaintiff Christian Kalled and the other members of the New Hampshire Subclass.

379. Defendants breached these representations and implied warranties. As described more fully above, Sony Online Services was not merchantable, fit for its intended purpose, and did not provide adequate security of Personal Information provided by New Hampshire Plaintiff Christian Kalled and the other members of the New Hampshire Subclass.

380. By virtue of its knowledge of the inadequate security of Sony Online Services, Defendants have received notice of the breach of the warranties.

381. By enacting N.H. Rev. Stat. Ann. § 382-A:2-318, New Hampshire eliminated both horizontal and vertical privity as defenses to implied warranty claims. Accordingly, the New Hampshire Subclass need not establish privity.

382. The damages suffered by New Hampshire Plaintiff and the other members of the New Hampshire Subclass were directly and proximately caused by the inadequate security of Sony Online Services and the resulting breach of implied warranties.

COUNT 31

**Negligent Misrepresentation Under New Hampshire Law
(On Behalf of New Hampshire Plaintiff Christian Kalled and the New Hampshire Subclass)**

383. New Hampshire Plaintiff Christian Kalled, individually and on behalf of the other members of the New Hampshire Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as though fully set forth herein.

384. Defendants negligently and recklessly misrepresented various material facts regarding the quality and character of Sony Online Services, in particular its security, although Defendants knew or reasonably should have known that the representations were not true. These misrepresentations were contained in online registration forms as well as various advertising, packaging, and correspondence from Defendants.

385. In reliance upon these misrepresentations about the security of Sony Online Services, New Hampshire Plaintiff Christian Kalled and the other members of the New Hampshire Subclass purchased the PS3s, PSPs, Sony Online Services and/or registered for Sony Online Services.

386. Had New Hampshire Plaintiffs and the other members of the New Hampshire Subclass, as reasonable persons, known of the inadequate security of Sony Online Services, they

1 would not have purchased PS3s, PSPs, Sony Online Services and/or registered for Sony Online
2 Services, or they would not have paid the prices they paid for same.

3 387. As a direct and proximate consequence of Defendants' negligent misrepresentations,
4 New Hampshire Plaintiff Christian Kalled and the other members of the New Hampshire Subclass
5 have suffered the injuries as alleged above.

6 **COUNT 32**

7 **Unjust Enrichment Under New Hampshire Law**
8 **(On Behalf of New Hampshire Plaintiff Christian Kalled and the New Hampshire Subclass)**

9 388. New Hampshire Plaintiff Christian Kalled, individually and on behalf of the other
10 members of the New Hampshire Subclass, hereby incorporates by reference the previous allegations
11 in paragraphs 1-145 as though fully set forth herein.

12 389. New Hampshire Plaintiff Christian Kalled and the other members of the New
13 Hampshire Subclass conferred a benefit on Defendants by purchasing PS3s, PSPs, Sony Online
14 Services and/or registering for Sony Online Services

15 390. Defendants have been unjustly enriched by the revenues from New Hampshire
16 Plaintiff Christian Kalled's and the other New Hampshire Subclass members' purchases of PS3s,
17 PSPs, Sony Online Services, and purchases of various games and downloads via Sony Online
18 Services. This enrichment is unjust and inequitable because Defendants misrepresented that Sony
19 Online Services had adequate security. Additionally, Defendants disabled access to Sony Online
20 Services after the Data Breach, rendering them unusable by subscribers. Moreover, by making these
21 misrepresentations, Defendants caused injuries to New Hampshire Plaintiff Christian Kalled and the
22 other members of the New Hampshire Subclass because: (a) they would not have purchased PS3s,
23 PSPs, Sony Online Services and/or registered with Sony Online Services on the same terms if the
24 true facts regarding the inadequate security of Sony Online Services were known; and (b) their PS3s,
25 PSPs, and Sony Online Services did not have the quality, security or value as promised.

26 391. Defendants' retention of the non-gratuitous benefit conferred on it by New Hampshire
27 Plaintiff Christian Kalled and the other members of the New Hampshire Subclass is unjust and
28

1 inequitable, and therefore Defendants must pay restitution to New Hampshire Plaintiff and the other
2 members of the New Hampshire Subclass, as ordered by the Court.

3 392. New Hampshire Plaintiff Christian Kalled and the other members of the New
4 Hampshire Subclass have no adequate remedy at law.

5 **COUNT 33**

6 **Violations of the New York Deceptive Practices Act, 7 New York General Business Law § 349 (On Behalf of New York Plaintiff Timothy Whyland and the New York Subclass)**

8 393. New York Plaintiff Timothy Whyland, individually and on behalf of the other
9 members of the New York Subclass, hereby incorporates by reference the previous allegations in
10 paragraphs 1-145 as though fully set forth herein.

11 394. This cause of action is brought by New York Plaintiff Whyland, individually and on
12 behalf of the New York Subclass, pursuant to the New York Deceptive Practices Act , New York
13 General Business Law (“GBL”) § 349.

14 395. Plaintiff Whyland and the other members of the New York Subclass are persons
15 within the meaning of GBL § 349(h). Defendants are engaged in business, trade or commerce or in
16 the furnishing of services within the meaning of GBL § 349(a).

17 396. GBL § 349(a) declares unlawful “[d]eceptive acts or practices in the conduct of any
18 business, trade or commerce or in the furnishing of any service in [New York State].”

19 397. As described herein, Defendants have engaged in consumer-oriented conduct that was
20 materially misleading and generally directed at the consuming public. The fundamental nature of
21 Defendants’ activity was to mislead the consuming public into believing that their Personal
22 Information would be safe upon transmission to Defendants when in fact Defendants knew that their
23 security systems were woefully inadequate.

24 398. New York Plaintiff Whyland and the other members of the New York Subclass have
25 been injured by Defendants’ deceptive acts and/or practices in that they have suffered the loss of
26 privacy and/or Personal Information and, further, have paid for PS3s, PSPs, Sony Online Services
27

1 and/or registered with Sony Online Services after exposure to Defendants' materially misleading
2 representations regarding the security of Sony Online Services.

3 399. Defendants willfully and/or knowingly violated GBL § 349.

4 400. The damages suffered by New York Plaintiff Whyland and the other members of the
5 New York Subclass were directly and proximately caused by the materially misleading acts and/or
6 practices of Defendants, as more fully described herein.

7 401. New Plaintiff Whyland and the other members of the New York Subclass have no
8 adequate remedy at law.

9 402. Pursuant to GBL § 349(h), New York Plaintiff Whyland, individually and on behalf
10 of the other members of the New York Subclass, seeks a court order enjoining the above-described
11 wrongful acts and practices of Defendants.

12 403. Pursuant to GBL § 349(h), New York Plaintiff Whyland, individually and on behalf
13 of the other members of the New York Subclass, seeks actual, statutory and treble damages, costs
14 and expenses, pre and post-judgment interest, and attorneys' fees.

15 **COUNT 34**

16 **Breach of Warranty Under New York Law** 17 **(On Behalf of New York Plaintiff Timothy Whyland and the New York Subclass)**

18 404. New York Plaintiff Timothy Whyland, individually and on behalf of the other
19 members of the New York Subclass, hereby incorporates by reference the previous allegations in
20 paragraphs 1-145 as though fully set forth herein.

21 405. The warranties and representations disseminated by Defendants regarding the security
22 of Sony Online Services were, and are, affirmations of fact and/or promises with regard to the
23 performance and quality of the product and/or service. These warranties and representations,
24 formed, in whole or in part, the basis of the bargain between Defendants and the members of the
25 New York Subclass, and constituted express warranties that Sony Online Services would conform
26 thereto. As described above, Sony Online Services did not conform with these warranties and
27 representations.
28

1 406. Defendants provided limited warranties to New York Plaintiff Whyland and the other
2 members of the New York Subclass, which Defendants breached and failed to honor. To the extent
3 there are any time and content limitations contained in those limited warranties, such limitations are
4 also unconscionable and grossly inadequate to protect the New York Plaintiff and the other members
5 of the New York Subclass. Among other things, members of the New York Subclass had no
6 meaningful choice in determining those time and content limitations; the terms of the limited
7 warranties unreasonably favored Defendants over members of the New York Subclass; a gross
8 disparity in bargaining power existed as between Defendants and members of the New York
9 Subclass; and Defendants knew Sony Online Services' security was inadequate and would fail to
10 provide the promised security.

11 407. By virtue of its knowledge of the inadequacy of Sony Online Services' security,
12 Defendants have received notice of the breach of the warranties.

13 408. The element of privity, if applicable, exists between Defendants and the members of
14 the New York Subclass because, *inter alia*: (i) Defendants have had direct written communications
15 with the members of the New York Subclass with regard to Sony Online Services in the form of
16 standardized warranty forms; (ii) members of the New York Subclass registered for Sony Online
17 Services directly with Defendants; (iii) Defendants marketed Sony Online Services to and
18 communicated directly with the New York Plaintiff and the other members of the New York
19 Subclass; and (iv) Defendants entered into contracts with the New York Plaintiff and the other
20 members of the New York Subclass in connection with the assurance of warranties.

21 409. As a result of the foregoing, New York Plaintiff Whyland and the other members of
22 the New York Subclass have suffered damages that were directly and proximately caused by the
23 inadequate security of Sony Online Services by Defendants.

COUNT 35

**Breach of Implied Warranty Under New York Law
(On Behalf of New York Plaintiff Timothy Whyland and the New York Subclass)**

410. New York Plaintiff Timothy Whyland, individually and on behalf of the other members of the New York Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as though fully set forth herein.

411. Defendants impliedly represented and warranted that Sony Online Services provided adequate security of Personal Information provided by New York Plaintiff Whyland and the other members of the New York Subclass.

412. Defendants breached these representations and implied warranties. Defendants made and/or allowed these misrepresentations to be made with the intent of inducing members of the New York Subclass to purchase PS3s, PSPs, Sony Online Services and/or register for Sony Online Services. If New York Plaintiff Whyland and the other members of the New York Subclass, as reasonable persons, known the true facts regarding the inadequate security of Sony Online Services, they would not have purchased PS3s, PSPs, Sony Online Services and/or registered for Sony Online Services, or they would not have paid the prices they paid for same.

413. By virtue of its knowledge of the inadequate security of Sony Online Services, Defendants have received notice of the breach of the warranties.

414. The element of privity, if applicable, exists between Defendants and the members of the New York Subclass because, *inter alia*: (i) Defendants have had direct written communications with members of the New York Subclass with regard to Sony Online Services in the form of standardized warranty forms; (ii) the New York Subclass members registered for Sony Online Services directly with Defendants; (iii) Defendants marketed Sony Online Services to and communicated directly with the New York Plaintiff and the other members of the New York Subclass; and (iv) Defendants entered into contracts with the members of the New York Subclass in connection with the assurance of warranties.

415. The damages suffered by the New York Plaintiff and the other members of the New York Subclass were directly and proximately caused by the inadequate security of Sony Online Services.

COUNT 36

Unjust Enrichment Under New York Law
(On Behalf of New York Plaintiff Timothy Whyland and the New York Subclass)

416. New York Plaintiff Timothy Whyland, individually and on behalf of the other members of the New York Subclass, hereby incorporates by reference the previous allegations in paragraphs 1-145 as though fully set forth herein.

417. New York Plaintiff Whyland and the other members of the New York Subclass had a direct relationship with Defendants and, in the course of that relationship, conferred a benefit on Defendants by purchasing PS3s, PSPs, Sony Online Services and/or registering for Sony Online Services and by providing their Personal Information to Defendants in doing so.

418. Defendants have been enriched in retaining the revenues derived from the New York Subclass members' purchases of PS3s, PSPs, Sony Online Services and/or registration on Sony Online Services, and purchases of various games and downloads via Sony Online Services, which retention under these circumstances is against equity and good conscience because Defendants misrepresented that Sony Online Services had adequate security. In addition, Defendants have been enriched by receiving and retaining the New York Plaintiff's and the other New York Subclass members' Personal Information, which receipt and retention under these circumstances is against equity and good conscience because Defendants misrepresented that Sony Online Services had adequate security.

419. Because Defendants' retention of the non-gratuitous benefit conferred on it by the New York Plaintiff and the other members of the New York Subclass is against equity and good conscience, Defendants must pay restitution to the New York Plaintiff and the other members of the New York Subclass for their unjust enrichment, as ordered by the Court.

420. New York Plaintiff Whyland and the other members of the New York Subclass have no adequate remedy at law.

COUNT 37

**Violation of the Ohio Consumer Sales Practices Act for Unconscionable Consumer Sales Practice, Ohio Rev. Code Ann. §1345.03
(On Behalf of Ohio Plaintiff James Wright and the Ohio Subclass)**

421. Ohio Plaintiff Wright, individually and on behalf of the other Ohio Subclass members, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

422. This cause of action is for damages and all other appropriate legal, injunctive and equitable relief for unconscionable consumer sales practice prohibited by the Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. §1345.03 on behalf of Ohio Plaintiff Wright and the other Ohio Subclass members.

423. Each of the following constitutes separate violations of Ohio Rev. Code Ann. §1345.03: (1) Defendants represented to Ohio Plaintiff Wright and the other Ohio Subclass members that Sony Online Services were adequately secure when in fact they were not; and (2) Defendants failed to honor the promise of adequate security for Sony Online Services; (3) Defendants offered Sony Online Services to Ohio Plaintiff Wright and the other Ohio Subclass members knowing that Sony Online Services did not have adequate security to protect their Personal Information from theft or misuse; (4) Defendants utilized the deceptive and misleading sales tactics to confuse and mislead Ohio Plaintiff Wright and the other members of the Ohio Subclass into providing their Personal Information to Defendants and into believing that Sony Online Services had adequate security to protect the Personal Information from theft or misuse.

424. Each representation and action described above is unconscionable in violation of Ohio Rev. Code Ann. §1345.03(A), and is specifically, among others and not limited to, in violation of: (1) Ohio Rev. Code Ann. §1345.03(B)(3) in that the Defendants knew at the time Ohio Plaintiff and the other members of the Ohio Subclass registered for Sony Online Services and provided their Personal Information to Defendants, that Sony Online Services were not adequate secure to protect the Personal Information from theft or misuse; (2) Ohio Rev. Code Ann. §1345.03(B)(6) in that Defendants knowingly made misleading statements of on which Ohio Plaintiff and the other members of the Ohio Subclass were likely to rely on to their detriment. These misleading statements

of opinion to Ohio Plaintiff Wright and the other Ohio Subclass members, which include but are not limited to the statement that Sony Online Services had adequate security to protect Personal Information from theft or misuse; and (3) Ohio Rev. Code Ann. §1345.03(B)(1) in that the Defendants took advantage of Ohio Plaintiff Wright and the other members of the Ohio Subclass by failing to adequately secure their Personal Information to protect against theft or misuse, knowing that Ohio Plaintiff Wright and the other Ohio Subclass members trusted Defendants that they would provide such adequate security.

425. As a direct and proximate result of Defendants' violation of Ohio Rev. Code Ann. §§1345.02(A), 1345.02(B)(3), 1345.02(6), and 1345.02(1), Ohio Plaintiff Wright and the other members of the Ohio Subclass have been damaged in an amount that will be proven at trial.

COUNT 38

Deceptive Trade Practice Under Ohio Law, Ohio Rev. Code Ann. § 4165.02 (On Behalf of Ohio Plaintiff James Wright and the Ohio Subclass)

426. Ohio Plaintiff Wright, individually and on behalf of the other Ohio Subclass members, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

427. This cause of action is for damages and all other appropriate legal, injunctive and equitable relief for deceptive trade practice under Ohio Rev. Code Ann. §4165.02, and has been brought by Ohio Plaintiff Wright, individually and on behalf of other members of the Ohio Subclass.

428. Each of the following constitute separate violations of Ohio Rev. Code Ann. §4165.02: (1) Defendants continuously represented during all relevant time periods that they had adequate security measures in place on Sony Online Services to protect Personal Information from theft or misuse, when in fact they did not; and (2) Defendants utilized deceptive and misleading print statements to confuse and mislead Ohio Plaintiff Wright and the other members of the Ohio Subclass to believe that Defendants had adequate security measures in place on Sony Online Services to protect Personal Information from theft or misuse, which they did not.

429. Such representations, individually and collectively, were made by Defendants in the course of their businesses, and in violation of Ohio Rev. Code Ann. §4165.02(A)(7), in that

1 Defendants represented that the security of Sony Online Services had characteristics, benefits, and
2 qualities that they did not have, namely that Sony Online Services had adequate security measures in
3 place to protect Personal Information from theft or misuse.

4 430. By making such representations, individually and collectively, Defendants willfully
5 engaged in a deceptive trade practice listed in Ohio Rev. Code Ann. §4165.02(A)(7), knowing it to
6 be deceptive.

7 431. Ohio Plaintiff Wright and the other members of the Ohio Subclass have been injured
8 as a direct and proximate result of Defendants' commission of a Deceptive Trade Practice listed in
9 Ohio Rev. Code Ann. §4165.02(A)(7), and were damaged in an amount that will be proven at trial.

10 **COUNT 39**

11 **Unjust Enrichment Under Ohio Law**
12 **(On Behalf of Ohio Plaintiff James Wright and the Ohio Subclass)**

13 432. Ohio Plaintiff Wright, individually and on behalf of the other Ohio Subclass
14 members, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully
15 set forth herein.

16 433. Ohio Plaintiff Wright and the other Ohio Subclass conferred a benefit on Defendants
17 by purchasing PS3s, PSPs, Sony Online Services and/or registering for Sony Online Services.

18 434. Defendants have been unjustly enriched in retaining the revenues derived from the
19 Ohio Subclass members' purchases of PS3s, PSPs, and Sony Online Services; registration for Sony
20 Online Services; and purchases of various games, music and downloads via Sony Online Services.
21 The retention of these benefits under the circumstances is unjust and inequitable because Defendants
22 misrepresented that Sony Online Services had adequate security. Moreover, by making these
23 misrepresentations, Defendants caused injuries to Ohio Plaintiff Wright and the other members of
24 the Ohio Subclass because: (a) as reasonable persons, they would not have purchased PS3s, PSPs,
25 Sony Online Services and/or registered with Sony Online services on the same terms if the true facts
26 regarding the inadequate security of Sony Online Services were known; and (b) their PS3s, PSPs,
27 and Sony Online Services did not have the quality, security or value as promised.
28

435. Because Defendants' retention of the non-gratuitous benefit conferred on it by Ohio Plaintiff Wright and the other members of the Ohio Subclass is unjust and inequitable, Defendants must pay restitution to Ohio Plaintiff Wright and the other members of the Ohio Subclass for their unjust enrichment, as ordered by the Court.

COUNT 40

Breach of Warranty Under Ohio Law (Common Law)
(On Behalf of Ohio Plaintiff James Wright and the Ohio Subclass)

436. Ohio Plaintiff Wright, individually and on behalf of the other Ohio Subclass members, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

437. Defendants, through their advertising and marketing, made uniform representations regarding the quality and adequacy of the security of Sony Online Services.

438. The representations made by Defendants were aimed directly at consumers including Ohio Plaintiff Wright and the other members of the Ohio Subclass, and induced Ohio Plaintiff Wright and the other Ohio Subclass members to register on, and provide their Personal Information to, Sony Online Services.

439. As a direct and proximate result of their reliance, Ohio Plaintiff Wright and the other members of the Ohio Subclass suffered damages in an amount to be proven at trial.

440. Defendants' standard and uniform representations in their advertising and marketing of Sony Online Services, including but not limited to that Sony Online Services had adequate security to protect Personal Information from theft or misuse, create a presumption of reliance as to the entire Ohio Subclass and obviates the need for individual proof of reliance.

COUNT 41

**Breach of Express Warranty Under Ohio Law,
Ohio Rev. Code Ann. § 1302.26
(On Behalf of Ohio Plaintiff James Wright and the Ohio Subclass)**

441. Ohio Plaintiff Wright, individually and on behalf of the other Ohio Subclass members, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

442. Through its uniform representations, Defendants made affirmations of fact and/or promises to consumers, including Ohio Plaintiff Wright and the other members of the Ohio Subclass, that Sony Online Services had adequate security to protect Personal Information from theft or misuse.

443. By making these affirmations of fact and/or promises to consumers, including Ohio Plaintiff Wright and the other members of the Ohio Subclass, the affirmations and/or promises became part of the basis for the bargain between Defendants and Ohio Subclass members who registered for Sony Online Services, and created an express warranty that Sony Online Services would conform to the affirmations and/or promises made by Defendants.

444. By failing to adequately secure Sony Online Services and to the Ohio Subclass members' Personal Information from theft or misuse, Defendants breached their express warranty to consumers who registered on the Network, including Ohio Plaintiff Wright and the other Ohio Subclass members

445. As a direct and proximate result of that breach, Ohio Plaintiff Wright and the other members of the Ohio Subclass suffered damages in an amount to be proven at trial.

COUNT 42

**Negligent Misrepresentation Under Ohio Law
(On Behalf of Ohio Plaintiff James Wright and the Ohio Subclass)**

446. Ohio Plaintiff Wright, individually and on behalf of the other Ohio Subclass members, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

447. In the course of its business dealings, Defendants had a duty to supply accurate and non-misleading information to Ohio Plaintiff Wright and the other members of the Ohio Subclass concerning the security of Sony Online Services. Further, Defendants had a duty to exercise reasonable care and competence in communicating the information about the security of Sony Online Services to Ohio Plaintiff Wright and the other members of the Ohio Subclass.

448. Defendants breached their duty and supplied false information to be used by Ohio Plaintiff Wright and the other members of the Ohio Subclass for their guidance in these consumer

1 transactions, namely that the Personal Information of Ohio Plaintiff Wright and the other Ohio
2 Subclass members would be secure on Sony Online Services, when in fact it was not.

3 449. This false information was justifiably relied upon by Ohio Plaintiff Wright and the
4 other Ohio Subclass members and induced them to register with, and send their Personal Information
5 to, Sony Online Services, thereby proximately causing them damages.

6 450. As a direct and proximate result of this reliance upon the false information, Ohio
7 Plaintiff Wright and the other Ohio Subclass members were damaged in an amount which will be
8 proven at trial.

9 **COUNT 43**

10 **Negligence Under Ohio Law**
11 **(On Behalf of Ohio Plaintiff James Wright and the Ohio Subclass)**

12 451. Ohio Plaintiff Wright, individually and on behalf of the other Ohio Subclass
13 members, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully
14 set forth herein.

15 452. By virtue of aforementioned acts of Defendants, Defendants in requesting, gathering
16 and promising to secure the Personal Information of Ohio Plaintiff Wright and the other Ohio
17 Subclass members had a duty to Ohio Plaintiff Wright and the other members of the Ohio Subclass
18 to do so in a reasonable manner consistent with industry standards, to ensure that Sony Online
19 Services were secure, and that Personal Information was secure from theft or misuse.

20 453. Defendants knew or reasonably should have known that Sony Online Services and the
21 Personal Information held on the Network was not secure.

22 454. Defendants breached their duty to of Ohio Plaintiff Wright and the other Ohio
23 Subclass members by failing to adequately secure Sony Online Services and placing their Personal
24 Information at risk of theft or misuse.

25 455. Defendant's negligence is independent of any contractual relationship between the
26 Defendants and Ohio Plaintiff Wright and the other Ohio Subclass members.
27
28

461. Tex. Bus. & Comm. Code § 17.46(c)(1) instructs that the TDTPA should be interpreted consistently with the constructions of Section 5(a)(1) the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) given by the Federal Trade Commission and federal courts.

462. Defendants have violated the TDTA by engaging in the unfair and deceptive practices as described above. Those practices contravene public policy and are immoral, unethical, unscrupulous and substantially injurious to consumers.

463. Plaintiff Christopher Wilson and the other members of the Texas Subclass have been injured by Defendants' unfair and deceptive practices in that they paid for PS3s, PSPs, Sony Online Services and/or registered for Sony Online Services after exposure to Defendants' false and misleading representations regarding the security of Sony Online Services.

464. The damages suffered by Plaintiff Christopher Wilson and the other members of the Texas Subclass were directly and proximately caused by the deceptive, misleading and unfair practices of Defendants, as more fully described herein.

465. Pursuant to Tex. Bus. & Comm. Code § 17.50(b)(2), Texas Plaintiff Christopher Wilson, individually and on behalf of the Texas Subclass, seeks a declaratory judgment and court order enjoining the above-described wrongful acts and practices of Defendants and for restitution and disgorgement.

466. Additionally, pursuant to Tex. Bus. & Comm. Code § 17.50(b)(1), (3) and 17.50 (d), Texas Plaintiff Christopher Wilson, individually and on behalf of the Texas Subclass, makes claims for restitution, disgorgement of all monies unlawfully obtained, actual damages, and attorneys' fees and costs.

COUNT 45

**Breach of Express Warranty Under Texas Law
(On Behalf of Texas Plaintiff Christopher Wilson and the Texas Subclass)**

467. Texas Plaintiff Christopher Wilson, individually and on behalf of the other Texas Subclass members, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

1 468. At all times relevant hereto, by advertising and selling PS3s, PSPs, and Sony Online
2 Services, Defendants made promises about the performance and quality of the security on PS3s,
3 PSPs, and Sony Online Services. Texas Plaintiff Christopher Wilson and the other members of the
4 Texas Subclass relied on these express warranties and representations in deciding to purchase PS3s,
5 PSPs, and Sony Online Services and/or registering for Sony Online Services, and these express
6 warranties and representations formed, in whole or in part, the basis of the bargain between
7 Defendants and Texas Plaintiff Christopher Wilson and the other members of the Texas Subclass.
8 As described above, the PS3, PSP, and Sony Online Services did not conform to these warranties
9 and representations.

10 469. Defendants provided limited warranties to Texas Plaintiff Christopher Wilson and the
11 other members of the Texas Subclass, which Defendants breached and failed to honor. In the event
12 that those limited warranties contain time and content restrictions, those limitations are
13 unconscionable and grossly inadequate to protect Texas Plaintiff Christopher Wilson and the other
14 members of the Texas Subclass. Among other things, Texas Plaintiff Christopher Wilson and the
15 other Texas Subclass members had no meaningful choice in determining those time and content
16 limitations; the terms of the limited warranties unreasonably favor Defendants over the members of
17 the Texas Subclass; there is a gross disparity in bargaining power between Defendants and the
18 members of the Texas Subclass; and Defendants knew Sony Online Services' security was
19 inadequate.

20 470. If Texas Plaintiff Christopher Wilson and the other members of the Texas Subclass,
21 as reasonable persons, known the true facts regarding the inadequate security of Sony Online
22 Services, they would not have purchased PS3s, PSPs, Sony Online Services and/or registered for
23 Sony Online Services, or they would not have paid the prices they paid for same.

24 471. Because Defendants knew of the inadequacy of Sony Online Services' security,
25 Defendants have received notice of the breach of the warranties.

26 472. As a result of the foregoing, Texas Plaintiff Christopher Wilson and the other Texas
27 Subclass members have suffered damages that were directly and proximately caused by the breach
28 of express warranties made by Defendants about the security of Sony Online Services.

COUNT 46

**Breach of Implied Warranties Under Texas Law,
Tex. Bus. & Comm. Code §§ 2.314, 2.315
(On Behalf of Texas Plaintiff Christopher Wilson and the Texas Subclass)**

473. Texas Plaintiff Christopher Wilson, individually and on behalf of the other Texas Subclass members, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

474. By creating, marketing, and selling PS3s, PSPs, and Sony Online Services, Defendants impliedly represented and warranted that Sony Online Services were merchantable, fit for their intended purpose, and provided adequate security of Personal Information provided by Texas Plaintiff Christopher Wilson and the other Texas Subclass members.

475. Defendants breached these representations and implied warranties. As described more fully above, Sony Online Services were not merchantable, fit for their intended purpose, and did not provide adequate security of Personal Information provided by Texas Plaintiff Christopher Wilson and the other Texas Subclass members

476. By virtue of its knowledge of the inadequate security of Sony Online Services, Defendants have received notice of the breach of the warranties.

477. Privity is established between Defendants and Texas Plaintiff Christopher Wilson and the other members of the Texas Subclass because Defendants have had direct written communications with Texas Plaintiff Christopher Wilson and the other members of the Texas Subclass with regard to Sony Online Services in the form of standardized warranty forms; the members of the Texas Subclass registered for Sony Online Services directly with Defendants; Defendants marketed Sony Online Services to and communicated directly with members of the Texas Subclass; and Defendants entered into contracts with members of the Texas Subclass in connection with the assurance of warranties.

478. The damages suffered by Texas Plaintiff Christopher Wilson and the other Texas Subclass members were directly and proximately caused by the inadequate security of Sony Online Services and the resulting breach of implied warranties.

COUNT 47

**Negligent Misrepresentation Under Texas Law
(On Behalf of Texas Plaintiff Christopher Wilson and the Texas Subclass)**

479. Texas Plaintiff Christopher Wilson, individually and on behalf of the other Texas Subclass members, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

480. In the course of their business, Defendants negligently and recklessly misrepresented various material facts regarding the quality and character of Sony Online Services and provided false information about the same, under circumstances where Defendants either knew or reasonably should have known that the representations were not true. These misrepresentations were contained in various advertising, packaging, and correspondence from Defendants, and such misrepresentations were further reiterated and disseminated by the officers, agents, representatives, servants, or employees of Defendants acting within the scope of their authority. Defendants did not exercise reasonable care and competence in communicating these representations to the members of the Texas Subclass.

481. In reliance upon these misrepresentations, members of the Texas Subclass purchased PS3s, PSPs, Sony Online Services and/or registered for Sony Online Services with the expectation that there was adequate security of Personal Information on the Sony Online Services.

482. Had the members of the Texas Subclass, as reasonable persons, known of the inadequate security of Sony Online Services, they would not have purchased PS3s, PSPs, Sony Online Services and/or registered with Sony Online Services, or they would not have paid the prices they paid for same.

483. As a direct and proximate consequence of Defendants' negligent misrepresentations, Texas Plaintiff Christopher Wilson and the other members of the Texas Subclass have been injured.

COUNT 48

**Money Had and Received / Unjust Enrichment Under Texas Law
(On Behalf of Texas Plaintiff Christopher Wilson and the Texas Subclass)**

484. Texas Plaintiff Christopher Wilson, individually and on behalf of the other Texas Subclass members, hereby incorporates by reference the previous allegations in paragraphs 1-145 as if fully set forth herein.

485. Texas Plaintiff Christopher Wilson and the other members of the Texas Subclass conferred a benefit on Defendants by purchasing PS3s, PSPs, Sony Online Services and/or registering for Sony Online Services.

486. Defendants have been unjustly enriched by the revenues from Texas Plaintiff Christian Kalled's and the other Texas Subclass members' purchases of PS3s, PSPs, Sony Online Services; registrations for Sony Online Services; and purchases of various games and downloads via Sony Online Services. This enrichment is unjust and inequitable because Defendants misrepresented that Sony Online Services had adequate security. Moreover, by making these misrepresentations, Defendants caused injuries to Texas Plaintiff Christopher Wilson and the other members of the Texas Subclass because: (a) as reasonable persons, they would not have purchased PS3s, PSPs, Sony Online Services and/or registered with Sony Online Services on the same terms if the true facts regarding the inadequate security of Sony Online Services were known; and (b) their PS3s, PSPs, and Sony Online Services did not have the quality, security or value as promised.

487. Defendants' retention of the non-gratuitous benefit conferred on it by Texas Plaintiff Christopher Wilson and the other members of the Texas Subclass is unjust and inequitable, and therefore Defendants must pay restitution to Texas Plaintiff Christopher Wilson and the other members of the Texas Subclass as ordered by the Court.

488. Texas Plaintiff Christopher Wilson and the other members of the Texas Subclass have no adequate remedy at law.

COUNT 49**Willful Violation of the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*
(On Behalf of Plaintiffs and all other Class Members)**

489. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1-145 above, as though fully stated herein.

490. FCRA creates a duty and requires consumer reporting agencies to adopt and maintain procedures for meeting the needs of commerce for consumer credit, personnel, insurance and other information in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. 15 U.S.C. § 1681(b).

491. FCRA defines a “consumer reporting agency” as:

Any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f).

492. FCRA defines a “consumer report” as:

[A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer’s eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b).

15 U.S.C. § 1681a(d)(1).

493. Sony, as defined herein, includes a series of separate entities, including SCEA, SNEA, SOE LLC, and SNEI, the defendants herein. On information and belief, on a cooperative basis, amongst various entities, Sony regularly engages, in whole or in part, in the practice of assembling information on consumers for the purpose of furnishing consumer reports to entities in the Sony group of companies, but separate and apart, and uses interstate commerce for the purpose of preparing and/or furnishing consumer reports or making available for inquiry such information to

1 entities other than those to which Plaintiffs and the other Class members provided their Personal
2 Information.

3 494. Sony was and is under a duty to adopt and maintain procedures designed to protect
4 and limit the dissemination of consumer credit and other information in a manner fair and equitable
5 to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of
6 such information. Sony, however, violated any duties owed by Sony pursuant to FCRA by failing to
7 adopt and maintain such protective procedures, which directly and/or proximately resulted in the
8 theft and wrongful dissemination of Plaintiffs' and the other Class Members' Personal Information
9 into the public domain, thus causing impermissible access and use.

10 495. Sony's violations of FCRA, as set forth above, were willful or, at the very least,
11 reckless.

12 496. As a direct and/or proximate result of Sony's willful and/or reckless violations of
13 FCRA, as described above, Plaintiffs' and the other Class Members' Personal Information was
14 stolen, compromised and made accessible to unauthorized third parties.

15 497. As a further direct and/or proximate result of Sony's willful and/or reckless violations
16 of FCRA, as described above, Plaintiffs and the other Class Members suffered (and continue to
17 suffer) damages in the form of, *inter alia*, (i) the untimely and/or inadequate notification of the Data
18 Breach; (ii) improper disclosure of their Personal Information; (iii) loss of privacy; (iv) out-of-pocket
19 expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon
20 them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity
21 fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of
22 their Personal Information, for which there is a well-established national and international market;
23 and (vii) rights they possess under FCRA—for which they are entitled to compensation.

24 498. Plaintiffs and the other Class Members, therefore, under FCRA, are entitled to
25 compensation for their actual damages including, *inter alia*, expenses for credit monitoring and
26 identity theft insurance, out-of-pocket expenses, and other economic and non-economic harm, or
27 statutory damages of not less than \$100, and not more than \$1000, per Class Member, as well as
28 their attorneys' fees, litigation expenses, and costs, pursuant to 15 U.S.C § 1681n(a).

COUNT 50**Negligent Violation of the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*
(On Behalf of Plaintiffs and all other Class Members)**

499. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1-145 above, as though fully stated herein.

500. Sony owed a duty to Plaintiffs and the other Class Members to safeguard and protect their Personal Information. In the alternative to Count 49, Sony negligently violated FCRA by failing to adopt and maintain procedures designed to protect and limit the dissemination and use of Plaintiffs' and the other Class Members' Personal Information for the permissible purposes outlined by FCRA, which directly and/or proximately resulted in the theft and wrongful dissemination of Plaintiffs' and the other Class Members' Personal Information into the public domain.

501. It was reasonably foreseeable that Sony's failure to maintain procedures to protect and secure Plaintiffs' and the other Class Members' Personal Information would result in an unauthorized third party gaining access to their Personal Information for no permissible purpose under FCRA. Sony's wrongful actions and/or inaction violated FCRA, as applicable.

502. As a direct and/or proximate result of Sony's negligent conduct, as described above, Plaintiffs' and the other Class Members' Personal Information was stolen, compromised and made accessible to unauthorized third parties and accessed by said third parties for no permissible purpose.

503. As a further direct and/or proximate result of Sony's negligent conduct, as described above, Plaintiffs and the other Class Members were (and continue to be) damaged in the form of, *inter alia*: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure of their Personal Information; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of their Personal Information, for which there is a well-established national and international market; and (vii) rights they possess under FCRA—for which they are entitled to compensation. Sony's wrongful actions and/or inaction violated FCRA, as applicable.

512. In contravention of the Settlement Agreement, Sony obtained Canadian plaintiffs' counsels' agreement to proceed with the Settlement Agreement separate from what was agreed to by the Settling Parties.

513. Even though the Settlement Agreement has been partially performed pursuant to Sony's demand, by their overt acceptance of the terms, Sony continues to refuse to act in accordance with good faith and fair dealing regarding attorneys' fees, costs, and expenses incurred and due in this litigation.

514. Sony has agreed to attorneys' fees, costs, and expenses for the Canadian cases.

515. In view of the agreement on all other terms, and the obligation to act in accordance with good faith and fair dealing, Plaintiffs herein seek, pursuant to the equitable powers of this Court, the enforcement of the Settlement Agreement and the determination of the attorneys' fees, costs, and expenses.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class members, respectfully request that this Court enter an Order:

A. Certifying the Class and State Subclasses under Federal Rule of Civil Procedure 23(a) and 23(b)(3), appointing Plaintiffs as Class Representatives, and appointing their undersigned counsel as Class Counsel;

B. Finding that Sony's conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

C. Enjoining Sony from engaging in the negligent, deceptive, unfair, and unlawful business practices alleged herein;

D. Awarding Plaintiffs and the other Class members actual, compensatory, and consequential damages;

E. Awarding Plaintiffs and the other Class members statutory damages;

F. Awarding Plaintiffs and the other Class members restitution and disgorgement;

G. Requiring Sony to provide appropriate credit monitoring and identity-theft prevention services to Plaintiffs and the other Class members;

H. Awarding Plaintiffs and the other Class members exemplary damages, should the finder of fact determine that Sony acted with oppression, fraud, and/or malice;

I. Awarding Plaintiffs and the other class members all applicable statutory damages in the amounts so provided by said statutes;

J. Awarding Plaintiffs and the other Class members pre-judgment and post-judgment interest;

K. Awarding Plaintiffs and the other Class members reasonable attorneys' fees and costs, including expert witness fees; and

L. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of all claims in this Consolidated Class Action Complaint so triable.

Dated: December 10, 2012

Respectfully submitted,

/s Paul J. Geller
PAUL J. GELLER
ROBBINS GELLER RUDMAN &
DOWD LLP
120 E. Palmetto Park Road, Suite 500
Boca Raton, Florida 33432
(561) 750-3000

/s Ben Barnow
BEN BARNOW
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, Illinois 60602
(312) 621-2000

/s Adam J. Levitt
ADAM J. LEVITT
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLC
55 West Monroe Street, Suite 1111
Chicago, Illinois 60603
(312) 984-0000

/s Brian R. Strange
BRIAN R. STRANGE (103252)
STRANGE & CARPENTER
12100 Wilshire Boulevard, Suite 1900
Los Angeles, California 90025
(310) 207-5055

/s David A. McKay
DAVID A. MCKAY
LAW OFFICES OF DAVID A. MCKAY LLC
555 North Point Center East, Suite 400
Alpharetta, Georgia 30022
(678) 366-5180

Plaintiffs' Steering Committee

1 /s Timothy G. Blood
2 TIMOTHY G. BLOOD (149343)
3 BLOOD HURST & O'REARDON, LLP
4 600 B Street, Suite 1550
5 San Diego, California 92101
6 (619) 338-1100

Plaintiffs' Co-Liaison Counsel

/s Gayle M. Blatt
GAYLE M. BLATT (122048)
CASEY GERRY SCHENK FRANCAVILLA
BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, California 92101
(619) 238-1811

CERTIFICATE OF SERVICE

I hereby certify that on December 10, 2012, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the email addresses denoted on the Electronic Mail Notice List, and that I shall cause the foregoing document to be mailed via the United States Postal Service to the non-CM/ECF participants indicated on the Electronic Mail Notice List.

/s Ben Barnow

BEN BARNOW
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, Illinois 60602
(312) 621-2000
b.barnow@barnowlaw.com